A LAYERED SOCIAL AND OPERATIONAL NETWORK ANALYSIS

THESIS

Jennifer L. Geffre, Captain, USAF

AFIT/GOR/ENS/07-07

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GOR/ENS/07-07

A LAYERED SOCIAL AND OPERATIONAL NETWORK ANALYSIS

THESIS

Presented to the Faculty

Department of Operational Sciences

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Operations Research

Jennifer L. Geffre, BS

Captain, USAF

March 2007

AFIT/GOR/ENS/07-07

A LAYERED SOCIAL AND OPERATIONAL NETWORK ANALYSIS

Jennifer L. Geffre, BS
Captain, USAF

Approved:

Richard F. Deckro, DBA, (Advisor)
Professor of Operations Research
Department of Operational Sciences

5 March 07
date

Shane A. Knighton, Maj, USAF (Reader)
Assistant Professor of Operations Research
Department of Operational Sciences

19 MAR 07
date

AFIT/GOR/ENS/07-07

Abstract

To provide maximal disruption to a clandestine/terrorist network's ability to conduct missions, we must develop a means to determine the individuals' importance to the network and operations. In a network centric world, this importance is represented as an additive value of their criticality across the convergence of multiple layers of network connections. The connections layers of the network are comprised of social layers (Acquaintance, Friendship, Nuclear Family, Relatives, Student-Teacher, and Religious Mentors, Reverent Power and others), as well as layers representing interactions involving Resources, Knowledge/Skills and Temporal Local. The social criticality of an individual is measured by centrality. Event Trees and Risk Importance Measures are often used in a system reliability analysis to determine critical elements in the success or failure of operations. The inclusion of time and location importance will be determined by the observation of various group members at that local. The synergy gained from the application of these concepts to terror groups can be used to identify critical locations, resources and knowledge to their operations and can then be attributed to individuals connected to those essential elements. The combination of social and operational criticality can then be used to identify individuals whose removal or influence would disrupt or diminish network operations.

To my husband, mom, brother, grandma and late grandpa

Acknowledgments

I would like to thank my family for the support to get through this trying time. Thank you to my husband for being my source of sanity and stability. Thank you to my mother, who will forever be my role model for strength and patience. Thank you to my brother, who always reminds me to laugh and puts things into perspective for me. Thank you to my grandma and grandpa for teaching me how to love and be loved. Without all of you this experience would have been far more difficult and not nearly as meaningful.

Words can not expression my gratitude to my committee members. Dr. Deckro, thank you kindly for the many hours of insightful discussion and guidance through this process. I am certainly coming to understand what "jade" is. Maj Knighton, thank you for willingness to take on an unfamiliar topic in the midst of helping so many of my classmates. It has been a joy to work with you both and I look forward to future opportunities to do so again.

Thank you also to Amy High for always making the time to help me. Your willingness to help me find the articles I needed and source documents made this process so much easier.

Finally, to my classmates who helped me through the more difficult times, especially toward the end, thank you! You have been friends in the truest sense and I am forever grateful for your kindness and the opportunity to have known and worked with you. I wish you the best as we venture forward and am hopeful our paths will cross again.

Jennifer L. Geffre

Table of Contents

List of Figures

List of Tables

1 Introduction

"Our war on terror begins with al-Qaida, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped and defeated"
– President G.W. Bush (2001)

1.1 Background

Since September 11, 2001 the face of conflict in the United States forever changed. The US now faces an adversary that is more technologically advanced and globally focused than ever before. The change in adversary organization, tactics and techniques has required the US to focus on strategies for combating terrorist organizations. The Department of State defines *terrorism* as:

> "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience" (2002: xvi).

To defeat these terrorist adversaries, the US must continue to develop methods for destabilizing their organizations. According to the 2006 release of the *National Strategy for Combating Terrorism*, the short term goals for the US must include the following (OPOTUS, 2006; 7):

- Kill or capture terrorists
- Deny them safe haven and control of any nation
- Prevent them from gaining access to Weapons of Mass Destruction (WMD)
- Render potential terrorist targets less attractive by strengthening security
- Cutting off sources of funding and other resources they need to operate and survive.

The purpose of this thesis is to create an approach for contributing to a network analysis that will assist in identifying critical individuals within clandestine networks.

The criticality of these individuals will depend on their resource connections and contributions to or influence within the network. Network resources will include *tangible* commodities, such as funding, and weapons or materials, while the *intangible* commodities will account for "knowledge, influence and social support" (Haythornthwaite, 1996).

The ideas of tangible and intangible commodities within a network can easily be seen in terror attacks conducted against US military members in Afghanistan and Iraq, as well as other locations throughout the world. An unconventional weapon utilized by terrorists in the region has been improvised explosive devices (IED). In hope of being able to prevent future IED attacks, the following questions should be used to identify critical elements or members of such an attack:

- Who is providing the money? – Funding is a critical element that perpetuates operations.
- Who has explosives training? – Specialized skills are needed to build IEDs and train others to build them.
- Who and Where are the IED materials coming from? – The originating point of the materials for such weapons will determine the best course of action to eliminate the source. The materials may be coming from other countries, other organizations, or from local weapons caches.
- Where are the IEDs being assembling? – The location of preparation and assembly of the weapons.
- Who is moving the weapon materials? – Typically, the middle men transport the raw materials.
- Who is commanding the attack and where are they meeting? – The organization's leadership provides oversight and direction. The location of their meetings and planning is vital.
- Who is placing or detonating the weapon? – The members who conduct attacks.

- What key infrastructure is likely to be targeted? – The location of potential targets.

The questions above provide the framework for identifying what is needed to destabilized the terrorist groups' operations. The *who* questions provide insight into the social relations between members and the resources or skills accessible to members. The *where* questions indicate the locations members frequent either for daily operations or for the planning and execution of an attack. The answers to these questions provide the information necessary to determine the critical members of the terrorist group and how best to attempt to destabilize their operations.

1.2 Problem Statement

The structure and operations of clandestine networks provide the opportunity for the use of various Operations Research techniques in order to gain insight into possible options to destabilize these networks. The nature of secrecy among clandestine networks makes the collection and development of perfect data nearly impossible. However, this research presents a methodology to identify critical members of a network, specifically a clandestine network, who if influenced or removed from the network could negatively impact terrorist operations or destabilize the network. The criticality of the individual members is based on their social connections, the tasks they contribute to, the skills and materials accessible to them, and their proximity to locations of importance.

1.3 Problem Approach

The position of this research is that current methods aimed at disrupting networks and their operations through the group's leadership are insufficient. Thus, a methodology

which considers the collective network, to include the operations, is needed to provide the best opportunity to destabilize these terrorist groups. This research provides a method which comprehensively analyzes a group's members through their social and operational contributions.

Though clandestine networks are not structured the same as other social networks, some SNA centrality measures concerned with the connections between members, rather than the hierarchy associated with power or influence, are appropriate for use. The weighted significance of different affiliations between group members indicates the *strength* of the relationship, the *distance* between members or the *likelihood* of a connection. The eigenvector centrality measures a member's importance based on the importance of the people he/she is connected to and has been found to be appropriate in scenarios with imperfect data. The extension of the eigenvector centrality to multidimensional scenarios provides a means to determine the importance of tasks and locations associated with the network's operations.

An organization's operations are comprised of multiple components which, predominately, work synergistically to complete tasks. In the context of terrorist groups, their operations take the form of attacks against weakened states, adversary military and government targets, and the civilian population. As with the preparations for any attack, there are potential components which will cause the attack to fail; this poses a risk to the terrorist group. The reliability of these components can then be modeled probabilistically in an event tree to determine the comprehensive risk of failure. Risk Importance Measures applied to the components of an attack identify and quantify the criticality of each component.

Finally, through a preference function, a criticality score is calculated for each member. The preference function is comprised of the member's criticality to the social network, operational effectiveness and location importance. These criticality measures are combined via a linearly weighted sum of the three factors. The higher the value calculated from a member, the more critical that member is to the operations and should be considered as a target for influence or removal from the network in order to destabilize the terrorist group and its operations.

1.4 Research Scope

The main focus of this research is on the terrorist networks that support these operations. It is recognized that other clandestine organizations, such as organized crime syndicates, drug and human trafficking groups and street gangs require similar operational networks. Investigations focused on these types of organizations would also benefit from the methodology presented in this research.

Additionally, this research focuses on the key operational tactics of al-Qaeda, as seen in recent attacks in Afghanistan, Iraq and throughout the world. The tactics specifically addressed in this research include suicide bombings and improvised explosive devices. Other considerations for tactics of interest include chemical, biological, radiological or nuclear (CBRN) weapons.

1.5 Assumptions

The assumptions incorporated into this methodology include the following:

- Analysts possess the means to collect and develop the social and operational intelligence related to the group of interest.

- The data collected is as complete and accurate as possible given the time constraints of the analysis.
- The social connections between members are undirected.
- The reliability or probabilities associated with the operational components can be found or calculated via historical data related to similar operations or attack tactics or from subject matter experts.
- All normalizations in this research use the one-norm.

1.6 Thesis Organization

Chapter 2 provides a review of supporting literature used in this thesis. Topics included in Chapter 2 focus on clandestine organizations, Social Network Analysis (SNA), risk and reliability analysis, and preference functions. Chapter 3 develops the methodology for determining member importance across the various layers of the network. This method explores the use of Social Network Analysis centrality, multidimensional centrality, risk analysis through event trees and risk importance measure, and weighted preference functions. Chapter 4 illustrates the methodology of this research by applying it to terrorist cells within al-Qaeda who were responsible for the US Embassy bombings in Kenya and Tanzania in 1998. Chapter 5 provides a summary of this research, as well as contributes potential extensions to the methods of this research.

2 Literature Review

2.1 Introduction

This chapter provides the foundation of literature used in development of the methodology of this research. The first focus is on organized crime and terror groups, their characteristics, structure, motivation, tactics, and strategies for destabilizing these groups. The section focusing on Social Network Analysis (SNA) includes various measures used in the sociological literature to calculate the importance or influence of members. The section also incorporates the use of Multi-dimensionality and Meta-Matrices. The next focus is on risk and its application to terrorist attacks through the use of event trees and risk importance measures. The final focus is on preference functions, the application of an additive linear model and techniques for determining weights.

2.2 Terrorism and Organized Crime

The emergence of a *new adversary* requires an understanding of who they are, how they are structured, what their motivations are, and what their tactics are in order to create methods to destabilize and disrupt their efforts. Since 2001, the US has come to understand that these new adversaries are unlike those of this nation's past; they are not a state to be attacked, they are not an army that can be distinguished from the civilian populace, their physical boundaries are limitless, their tactics are unconventional and their operations are supported by modern technology and connectivity unheard of in the past. The current focus of the US is on "transnational extremist organizations, networks and individuals" (OPOTUS, 2006: 5). These transnational threats, which compromise the security of the US, consist of terrorists groups, organized crime syndicates, the trafficking

of drugs and illegal aliens and the smuggling of Weapons of Mass Destruction (WMD) (National Defense University, 1999:245).

While the adversary is more difficult to discern from the civilian population, these *covert* or *clandestine* networks behave differently than most *social* networks (Baker and Faulkner, 1993: 843). The characteristics of a *clandestine* organization, which distinguish it from civilian social networks, are identified by three factors (McCormick and Owen, 2000:177):

1. Group Size – The number of members in each cell and the number of cells
2. Group Structure - The number and nature of communications/relations between the group's cells.
3. Group Location – The cells location in proximity to adversary's center of gravity.

These characteristics aid the group in their ability to draw attention to their operations. The ability to control the group's size, structure and location, create the opportunity to effectively work undetected.

Clandestine networks, terrorist or otherwise, depend on the secrecy for existence. McCormick and Owen suggest that the "survival" of such an organization depends on their "invisibility" (2000: 175). They suggest this can be accomplished one of two ways, through the "organizational capacity…or level of operational security" (McCormick and Owen, 2000:175-176). Rules too stringent on the size of the group or the procedures for operational security (OPSEC), severely limit the successfulness of the group. Therefore a balance between secrecy and operational communications is vital (Baker and Faulkner, 1993: 843).

While the motivations of the terrorist groups and organized criminals differ, the similarities between them enable analysis methods to be applied with limited differences. This is due to the nature of the organizations and their operations methods, as they are more similar than different (Sanderson, 2004:49). Through various sources, Sanderson has compiled several similarities between terrorist groups and organized criminal groups, as seen in Table 1 (2004: 53).

Table 1 - Characteristics of Organized Crime and Terrorist Groups (Sanderson, 2004: 53)

Similarities between Organized Crime and Terror

Descriptors	Actions
▪ Are rational actors	▪ Use violence or threat of reprisal
▪ Have "interchangeable" recruitment pool	▪ Use kidnapping, assassination and extortion
▪ Are adaptive, innovative and resilient	▪ Pose asymmetrical threat to US and allies
▪ Have back-up leaders and foot soldiers	▪ Members rarely allowed to leave, often fatal
▪ Secret Operations, Covert	▪ Defy the state and rule of law (unless state sponsored)
	▪ Provide social services in community

2.2.1 Structure

To understand these clandestine groups, knowledge of this underlying structure is imperative to providing insights. Since groups of terrorist and/or organized crime are different, the strategies for dealing with each will vary. The structure of terror, as described in the *National Strategy for Combating Terrorism*, is comprised of five components seen in Figure 1 (OPOTUS, 2003: 6).

Figure 1 - Structure of Terror (OPOTUS, 2003: 6)

These underlying conditions are based on the real and perceived grievances of the group. The international environment and states are related in the role of enabling the group to operate knowingly or in being unstable enough for the group to operate without resistance. The organization is meant to carry out the strategies and direction of the leaders.

The components of the terror structure are not unique to terror groups; they can be seen in organized crime as well. Crime groups consist of "complex, clandestine, hierarchically organized networks" (National Defense University, 1999: 256). Corruption is an effective mechanism to continue operations unhampered in portions of the US and abroad. This corruption can thrive only in an areas were government officials and police can be influenced (National Defense University, 1999: 250).

Unlike the hierarchically structure of organized crime groups, the *new* terror groups work in clusters or cells. This "compartmentalized" structure refers to the distinct tasks, operations and logistics support (Sageman, 2004: 170). Members of a specific cell are often highly inter-connected, but have limited connections beyond the cell (Sageman, 2004:170; Krebs, 2002: 46-49). This structure is effective for a number of reasons. The first being the "minimized damage" to the total network should a single cell be

jeopardized (Krebs, 2002: 46). Another benefit to the organization is the difficulties associated "identifying, locating and eradicating" small, highly dispersed cells (National Defense University, 1999: 249).

As mentioned in the previous section, the OPSEC practices of a group complement the structure of the organization. OPSEC measures provide guidance for members with regard to topics that can be discussed, means of communications, protection of identity, and security practices associated with various aspects of operations. The *al-Qaeda Training Manual* describes the security measures for the use of forged identification, safe houses, methods of communication, means of transportation, and codes or ciphers for encrypting messages (Post, 2005). Though these protective measures are extensive, they are also dynamic; they must continue to adapt their security as their adversary threatens the organizations operational success.

2.2.2 Small-World Theory

The six degrees of separation concept is familiar to most analysts and even those outside of the mathematical and scientific communities. Its popularity is attributed to Stanley Milgram, whose research in the mid-1960's produced the theory that people of the world are interconnected through a maximum of six other people. Granovetter describes a world in which personal relations are either *strong ties* or *weak ties* (1973: 1360). The *strong ties* correspond to one's close relations, family, friends, or co-workers. The *weak ties* are the relations we spend limited time with, acquaintances.

A world built only on strong ties, creates many isolated groups. It is only the addition of the weak ties to a network that limits the separations between the interconnected clusters (Buchanan, 2002: 55). The density of the strong ties in a cluster

makes the removal of such a relation nearly ineffective, however the removal of a weak tie has the potential to detach otherwise isolated groups (Buchanan, 2002: 41-42). This concept is especially interesting in the context of destabilizing network operations.

There are two essential pieces to these large networks, *hubs* and *weak ties*. First, the individuals who are well connected within a large network typically create a link between isolates (Sageman, 2004: 164). These *hubs* are essential to the network, as communications must pass through them to get to the isolates, thus creating "vulnerabilities" within the network (Sageman, 2004:164, 141). Second, *weak ties* provide the opportunity for recruitment into the group. Without these *weak ties* the isolated groups of family and friends would join without the potential for outsiders to also join (Sageman, 2004: 169).

While the hubs create an opportunity to impact the networks, especially if the removal of multiple hubs were considered at the same time, there are few options available to compensate for weak ties. These weak ties generally result from chance meetings and may not be commanded by the leaders, which adds a level complexity when trying to break those ties. If, however, known locations or occasions exist for recruiting (i.e. particular meetings, a specific conference, or a specific mosque or church) the observation and detection of weak ties may be improved. An additional complication resulting from the clandestine nature of the group is the appearance of weak ties where strong ties actually exist (Krebs, 2002:49).

2.2.3 Motivation

Terrorist groups and organized crime groups differ significantly in their goals and motivation for their cause. The focus of criminal groups is money; the trafficking of

drugs or people, the money laundering, and the corruption are a means to generate more money (National Defense University, 1999: 249-250). While the terrorists participate in similar activities to generate funds, this is a necessity to achieve their religious and ideological goals (National Defense University, 1999: 256; Sanderson, 2004: 55).

The ideological goals of the jihadist terrorist groups are meant to further separate the Muslim and Non-Muslim communities throughout the world (OPOTUS, 2006: 5). As seen most recently in Afghanistan and Iraq, the goals have been to "overthrow civil order and replace freedom with conflict and intolerance" (OPOTUS, 2006: 5). Specifically, al-Qaeda has three primary goals (Moghaddam, 2006: 4-6):

1. Complete US withdraw from the Muslim region
2. Halt of US support to Israel
3. Halt to US support and manipulation of countries like Saudi Arabia and other in the region

Only once these motivations are understood, can the US and its allies combat these terrorists.

2.2.4 Tactics

Understanding the tactics of a group provide insight which allow opportunities to be developed to defeat the group. The tactics implored by a group are determined by the personnel and materials within their control. The motivation of the group is also an indicator of the type of tactics the group is likely to use.

As mentioned in the previous section, organized crime groups operate utilizing corruption to create the environment for illegal financial activities. When coercion or bribery is ineffective, assassination is used (National Defense University, 1999:250).

Economic and industrial espionage, bank fraud, financial market manipulation, and counterfeiting are aided by electronic fund transfers and further promote the financial goals of the groups (National Defense University, 1999:250).

The tactics employed by terror groups focus on creating a conducive environment and operational opportunities aimed at achieving their goals. First, the groups prey on states with struggling governments. The weakened states lack the capability to resist the terrorists. The unstable environment allows terrorists to create networks of safe houses, logistics trails, and a population to begin recruiting (Takeyh and Gvosdev, 2002: 98). Next, the tactics, with respect to the operations, include decisions about target selection and weapons selection. Attacks focus on government and political buildings, financial, religious and large public areas, and the people in these areas. These attacks may be carried out by suicide bombings, conventional weapons, improvised explosive devices, and chemical, biological, radiological and nuclear weapons. The targets are selected to destabilize weakened states and spread fear among the targeted population.

The number of suicide bombings across the world has increased dramatically, especially in Afghanistan (Department of the State, 2006; Maples, 2007). Suicide bombings are meant to instill fear in the public and coerce the government/adversary to comply (Pape, 2003:344). Suicide bombings are a tactic of choice for groups with limited resources (Moghaddam, 2006: 123). They are inexpensive, except for human capital, yet highly effective – making a "suicide terrorists the ultimate smart bomb" (Hoffman, 2003) or the "guided missiles of poor armies" (Moghaddam, 2006: 125).

Explosive devices can be either conventional weapons or improvised from a number of sources such as munitions, home made explosives or some combination of

easily available explosives. The conventional munitions include small arms, rocket propelled grenades, and so forth. The improvised explosive devices (IED) are often home made from either advanced or rudimentary materials. The IEDs may be more substantial if supplied by a third party group. The IEDs can be implanted, in the open or placed in vehicles; they may be pressure, time, command wire or remote sensor detonated; they may be individual or linked together (daisy-chain) (MNF-I, 2007).

The chemical, biological, radiological, and nuclear (CBRN) weapons are one of the nation's most significant concerns (OPOTUS, 2006: 7). There are various sources of chemical and biological agents, with numerous means of deployment. Radiological and nuclear materials are likely to surface as a "dirty bomb", as rudimentary materials are "more accessible and less expensive" (Stanislawski and Hermann, 2004) and do not require the advanced skills need to arm a nuclear warhead.

2.2.5 Disrupt/Destabilize

Ultimately the efforts attributed to understanding the structure, motivations, and tactics of a group are used to disrupt or destabilize the network. Carley *et al.* suggest that destabilization occurs when the resources, communications, and workload are impacted (2003: 4). People who are well connected, the *hubs*, are ideal choices (Carley *et al.*, 2003:4; Klerks, 2001:62). Another option is to target those who attain expertise or provide goods (Carley *et al.*, 2003:4; Klerks, 2001:62, Krebs, 2002:50).

2.3 Social Network Analysis

The study of social networks has evolved since the early 1930's and has come to incorporate the sciences of anthropology, social theory, mathematics, statistics, and

computers (Wasserman and Faust; 1994: 10) and more recently, operations research. Foundations of this growing field are based in the theory and notation of graphs, sociometrics and algebra (Wasserman and Faust, 1994: 69-82). There are three topics of particular interest, which can be answered through Social Network Analysis (SNA) (Tichy *et al.*, 1979: 509):

1. Transactional Content: The "exchange" between members,
2. Nature of Links: The "strength and quality" of connection between members,
3. Structural Characteristics: The "pattern of relations" among members.

An important aspect of SNA as opposed to other approaches, is the focus on the "structure of the network" instead of the "characteristics of the individuals" in the network (Ressler; 2006).

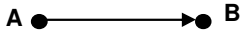
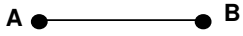
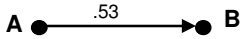
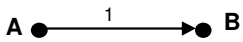
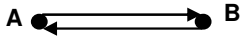
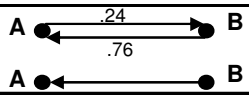
The remainder of this section is focused on specific measures, applications of, and advances in SNA. Centrality provides a means to determine a network member's importance. Multidimensional centrality applies a centrality measure across network layers or time and location information associated with a network. Finally, advances in data representation for analysis beyond simply the social ties within a network are available via meta-matrices.

2.3.1 Centrality

There is no standard, nor overarching agreement between those in the social network community as to what constitutes centrality or even how it is quantified (Freeman, 1979: 217). Centrality has been known as several concepts over the years, including: prestige, influence, prominence, importance. Roughly, centrality is associated with members who are near the "structural center" of a network and are typically seen as

being in a special position (Freeman, 1979: 218). The type of network or graph determines the measure of centrality considered most appropriate. The concepts and terms important in networks, graphs, and centrality are included in Table 2 (West, 2001:520-532).

Table 2 - Graph Theory terms for SNA

Term	Definition	Example
Directed	An edge or set of edges, which designate a head and a tail	
Undirected	An edge or set of edges, which does not distinguish a head or tail	
Weighted	An assigned value of distance or strength to an edge	
Unweighted	An edges whose weight is one; edges without a value are assumed to be one	
Symmetric	Implies if A can reach B, that B can reach A equally	
Asymmetric	Does not assume that A and B can be reached equally	

The centrality measures use several other terms, which must be examined in order to define and calculate each measure. *Adjacency* describes a connection between to members. *Degree* is based on the number of members to which a specific member is adjacent. A *path* identifies a sequence of adjacencies between two members via intermediary members. *Distance* is the number of adjacencies in a path. Finally, a *geodesic* is a path with the shortest distance. With the understanding of these terms, degree, closeness, betweenness, information centralities can be defined. This section also discusses are eigenvector centrality and Katz's influence measure.

The basics of degree centrality are found in the definition of degree. Freeman explains degree centrality as an individual who is highly "visible" or is in a position with the "potential for activity". Degree centrality is typically applied to undirected graphs

and since the measure is based on the simple adjacency, weighting on the edges are disregarded; though can be used as in-degree or out-degree for directed graphs. This measure is seen as the ability for a person to influence those directly connected to them (Borgatti, 2005: 62). Hence a person with many connections will have a higher score than one with few connections. An individual's degree centrality can be calculated via Equation (2.1); the column sum of an adjacency matrix (Wasserman and Faust; 1994: 178).

$$C_D = \sum_j x_{ij} \tag{2.1}$$

Sade argues that 1-step degree centrality does not contain enough information about the relationships of a network; 2 or 3-step in-degree, up to paths of no more than 10 should instead be considered (1989: 281).

Closeness provides a measure based on an individual's distance to all other members of the network (Sabidussi, 1966: 587-588). The measure will have varied results based on the directedness, weighting, and symmetry of the graph. Borgatti asserts that low scores indicate a shorter distance between members, also corresponding to the individuals most likely to receive information the soonest (2005: 59). This closeness is scored as the inverse of the sum of the shortest path from a member to all others, as depicted in Equation (2.2); here $d(n_i, n_j)$ represents the distance from member i to member j and g is the number of members in the group (Wasserman and Faust, 1994: 184).

$$C_C\left(n_i\right) = \left[\sum_{j=1}^{g} d\left(n_i, n_j\right)\right]^{-1} \tag{2.2}$$

Betweenness, while similar to closeness, utilizes the shortest paths between all members. The calculation accounts for the proportion of times member *k* is an intermediary on the shortest paths between all members *i* and *j* to the total number of shortest paths between the all members. A high betweenness value for a member indicates a potential for influence on the interactions between members, who are dependent on intermediaries for connections (Wasserman and Faust, 2001: 188) or have the "control" to "shut off" communication flow (Borgatti, 2005: 60). Again, the directedness, symmetry and weighting of the graph will limit the possible paths and thus the value a member earns. The calculation for betweenness is seen in Equation (2.3) (Wasserman and Faust; 1994: 190).

$$C_B(n_i) = \sum_{j<k} \left(\frac{g_{jk}(n_i)}{g_{jk}} \right) \tag{2.3}$$

Information centrality is yet another measure similar to closeness and betweenness. However, it is purported that information and communications do not adhere to a short path to flow through a network (Stephenson and Zelen, 1989: 3). Information centrality differs in that it accounts for the number of times member *k* is on any path between members *i* and *j*, not just the shortest path. For an unweighted graph, Equation (2.6) determines an individual's information centrality (Stephenson and Zelen, 1989: 12). The matrix $B = (b_{ij})$ is based on (2.4) and (2.5).

$$b_{ij} = \begin{cases} 0 & \text{points } i \text{ and } j \text{ are incident} \\ 1 & \text{otherwise} \end{cases} \tag{2.4}$$

$$b_{ii} = \{1 + \text{ degree of point } i \tag{2.5}$$

Let $C = \left(c_{ij}\right) = B^{-1}$, $T = \sum_j c_{jj}$, $R = \sum_j c_{ij}$. Then, the information centrality of member *i* is given in Equation (2.6).

$$I_i = \left(c_{ii} + \frac{\left(T - 2R\right)}{n} \right)^{-1} \tag{2.6}$$

An alteration made for weighted graphs is seen in (2.7) (Stephenson and Zelen, 1989: 14).

$$b_{ij} = \begin{cases} \left(1 - \text{ weight of line connecting points } i \text{ and } j\right) \\ 1 \quad \text{if points } i \text{ and } j \text{ are not adjacent} \end{cases} \tag{2.7}$$

Hamill suggests using caution with this centrality measure, as a flaw in the counting of all possible paths creates a difference in values based on a heuristic and the above method; he also explains that using *all* possible paths as given in the problem definition by Stephenson and Zelen, corrects the error (2006: 304).

Finally, the eigenvector centrality developed by Bonacich *et al.* considers a member's importance based on the importance of the members to whom he is connected.

> Definition 1: Let A be an *n* by *n* matrix. Then an *eigenvalue* is a scalar, λ, associated with a non-trivial solution (where $x \neq 0$) to the equation $Ax = \lambda x$ (Kincaid and Cheney, 2002: 255).
>
> Definition 2: The non-zero vector, *x*, which satisfies $Ax = \lambda x$ is the *eigenvector* of A corresponding to the eigenvalue λ (Kincaid and Cheney, 2002: 255).

Equation (2.8) represents the eigenvector calculation, were *A* is the adjacency matrix, λ is the largest positive eigenvalue, and *v* is the eigenvector associated with the largest eigenvalue (Bonacich, 1987: 1172).

$$\lambda v = Av \tag{2.8}$$

For this method of centrality to be applied to asymmetric graphs, the addition of an attenuation factor $\alpha < (1/\lambda)$ and *e* as a vector of ones, the resulting calculation is (2.9) (Bonacich and Lloyd, 2001: 196).

$$v = \left(I - \alpha A^T\right)^{-1} e \tag{2.9}$$

Newman expanded this method to incorporate the use of edge weights in the matrix in place of the one, representing adjacency (2004: 056131-2). This concept has been associated with PageRank, an algorithm used by search engines on the internet to rank sites based on the *importance* of the site links imbedded in a specific page (Newman, 2004: 056131-2).

As early as 1953, Katz established a measure meant to determine one's "status, influence or transmission of information" (1953: 39). This measure hinges on an attenuation factor, which Katz describes as attributing a "lower effectiveness of longer chains"; providing long paths with smaller values (1953: 40). This attenuation factor, α, is found via the largest eigenvalue (λ_1) for the adjacency matrix *C*. Then $\frac{1}{\alpha}$ is the integer on the interval $\lambda_1 \le \frac{1}{\alpha} \le 2\lambda_1$ (Katz, 1953: 42). In this construction, *s* is also needed, the column vector of row sums of *C'*, such that $s = C'u$; where *u* is a vector of ones. Equation (2.10) shows the individual contributions to the influence measure (Kats, 1953: 41).

$$t = \left(\frac{1}{\alpha} I - C'\right)^{-1} s \tag{2.10}$$

This vector is then scaled by the constant *m*, as in (2.11) (Katz, 1953: 42).

$$m = (n-1)!\alpha^{(n-1)}e^{(1/\alpha)} \tag{2.11}$$

The Katz influence measure is given by the product $\frac{1}{m}t$.

2.3.2 Multidimensional Centrality

Bonacich *et al.* determined a method for incorporating triad relationships, time, and location into social network studies. Utilizing the basic eigenvector centrality, the method can analyze relations across multiple dimensions (Bonacich *et al.*, 2004: 189). Bonacich *et al.*, use adjacency matrices or node-arc incidence matrices depending on the data and objective of the analysis. A node-arc incidence matrix creates a row based on a single connection, while the columns represent the members. A row is filled by placing a one in columns corresponding to those with the connection, and zero is the remaining columns. Bonacich *et al.* augments the adjacency or incidence matrices to include time and location information.

Figure 2 shows a set of relationships between four members, at three separate points in time.

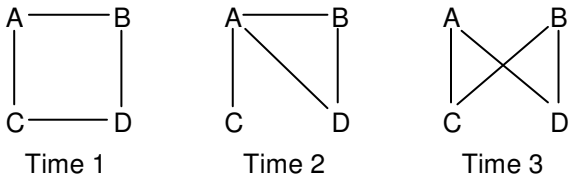


Figure 2 - Four Members at Three Points in Time

The corresponding augmented node-arc incidence matrix is represented in Table 3.

Table 3 - Four Member/Three Times Matrix

	Members				Time		
	A	B	C	D	1	2	3
A-B	1	1	0	0	1	0	0
A-C	1	0	1	0	1	0	0
B-D	0	1	0	1	1	0	0
C-D	0	0	1	1	1	0	0
A-B	1	1	0	0	0	1	0
A-C	1	0	1	0	0	1	0
A-D	1	0	0	1	0	1	0
B-D	0	1	0	1	0	1	0
A-C	1	0	1	0	0	0	1
A-D	1	0	0	1	0	0	1
B-C	0	1	1	0	0	0	1
B-D	0	1	0	1	0	0	1

Let the matrix in Table 3 equal *E*, then let $A = E^T E$ and find the eigenvector associated with the largest eigenvalue of A. The eigenvector and normalized eigenvector of member and time importance are shown in Table 4. These results show that member A holds the highest centrality score and that Time 3 was most important.

Table 4 - Multi-Dimensional Centrality Score

		Eigenvector Centrality	Normalized Eigenvector Centrality
Members	A	0.52	0.30
	B	0.43	0.25
	C	0.34	0.20
	D	0.43	0.25
Time	1	0.30	0.29
	2	0.28	0.28
	3	0.44	0.43

2.3.3 Meta-Matrix

Carley has created a method for depicting the many diverse aspects of a network through the use of *meta-matrices*. A meta-matrix conveniently combines the inter-relationships between the members, knowledge, resources, tasks and organization affiliation (2001, 2002). A variety of measures can be applied to the various submatrices within the meta-matrix (Carley, 2001: 1). Table 5 depicts a meta-matrix with the components of importance to this research (Carley *et al.*, 2006: 85).

Table 5 - Meta-Matrix Relations (Carley, 2001: 2)

	Member	Knowledge	Resources	Tasks
Member	**Communications Network** *Who knows who*	**Knowledge Network** *Who knows what*	**Capabilities Network** *Who has what resource*	**Assignment Network** *Who does what*
Knowledge		**Information Network** *What informs what*	**Training Network** *What knowledge is need to use which resource*	**Knowledge Requirements Network** *What knowledge is needed to do the task*
Resources			**Resource Substitution Network** *What resources can be substituted for which*	**Resource Requirements Network** *What resources are needed to do that task*
Tasks				**Precedence Network** *Which task must be done before which*

Carley suggests four measures likely to destabilize terrorist networks: degree, betweenness, cognitive load, and task exclusivity (2003: 5). The meta-matrix analysis software developed by the Computational Analysis of Social and Organizational System is Organizational Risk Analyzer (ORA) which calculates each of the measures in Table 5 provides a brief definition, sub-matrix used, and explanation of the calculation for each measure of interest (Carley, 2002:5; 2004: 18-29).

Table 6 - ORA Measures using Meta-Matrices

Measure	Definition	Sub-Matrix	Calculation	Reference
Degree Centrality	Number of connections member has	M/M	Normalized row or column sums	Carley and Reminga (2004: 30)
Betweenness Centrality	The proportion of shortest paths that use a member as an intermediary	M/M	Normalized Equation (2.3)	Carley and Reminga (2004: 30)
Cognitive Load/ Demand	Amount of effort expended to complete a task	M/R & R/T or M/K & K/T	Average of 6 measures based on (M/T * R/T') or (M/T * M/T')	Carley and Reminga (2004: 22)
Task Exclusivity	Detects members who exclusively perform tasks	M/T	$\sum_{j=1}^{\lvert T\rvert} MT(i,j) * \exp\left(1 - sum\left(MK(:,j)\right)\right)$	Carley and Reminga (2004: 28)

M/M - Member/Member, M/K - Member/Knowledge, M/T - Member/Task,
M/R - Member/Resource, R/T - Resource/Task, K/T - Knowledge/Task

2.4 Modeling Operations with Probabilistic Risk Analysis

While many in the US and other nations are using risk analysis to minimize the impact of terrorist attacks, viewing attacks or operations from the perspective of the

terrorist groups provides additional opportunities for analysis. Due to limited resources available to terror groups and their desire to conduct successful attacks, the concepts of extreme events can be applied, as a failure would be considered an "unacceptable risk" (Haimes, 2004: 300). This can be attributed to any number of components which contribute to the success or failure of their operations. Probabilistic Risk Analysis (PRA) can be applied to: system analysis, containment analysis and/or consequence analysis.

2.4.1 Risk

The Department of Defense defines *risk* as the "probability and severity of loss linked to hazards" (DoD Dictionary, 2001). Kaplan and Garrick consider the following as the basis for their definition, Risk = Uncertainty + Damage (1981:12). Risk is an area of research widely applied across various disciplines, such as system and human reliability and project management (Bedford and Cooke, 2001; Høyland and Rausand, 1994). These disciplines are most concerned with the uncertainty of events and mitigation measures taken to reduce the threat or risk.

Kaplan and Garrick define risk as a triplet, Equation (2.12):

$$R = \left\{ \left\langle S_i, L_i, X_i \right\rangle \right\} \tag{2.12}$$

S_i represents a risk scenario, L_i is the likelihood of the scenario and X_i is the outcome associated with the scenario (1981: 13). To better enable identification of all possible risk scenarios associated with a system or project, Kaplan and Garrick suggest the following questions (1981: 13):

What can go wrong? $\rightarrow S_i$
How likely is it to happen? $\rightarrow L_i$
What are the consequences? $\rightarrow X_i$

The risk triplet can be applied to the context of group operations. The risk scenarios in this study are associated with the reliability, availability or quality of materials, the availability or level of expertise and the possibility of detection or interference by the adversary. The likelihood is a probability associated with success or level of the materials, expertise and/or adversary actions. Finally, the consequences are considered in terms of system or operations success or failure. The cause of a failure is described later.

2.4.2 Event Tree/Reliability

Event trees provide the framework for the visualization of "forward logic" (Bedford and Cooke, 2001: 99). The tree begins with an initiating event and grows as combinations of system influencing components are incorporated (Bedford and Cooke, 2001: 99). The components are modeled sequentially, allowing the outcome likelihoods to be quantified (Papazoglou, 1998: 169-170). Figure 3 shows an example of an Event Tree, which will be used through the remainder of this section to explain concepts and analysis techniques.

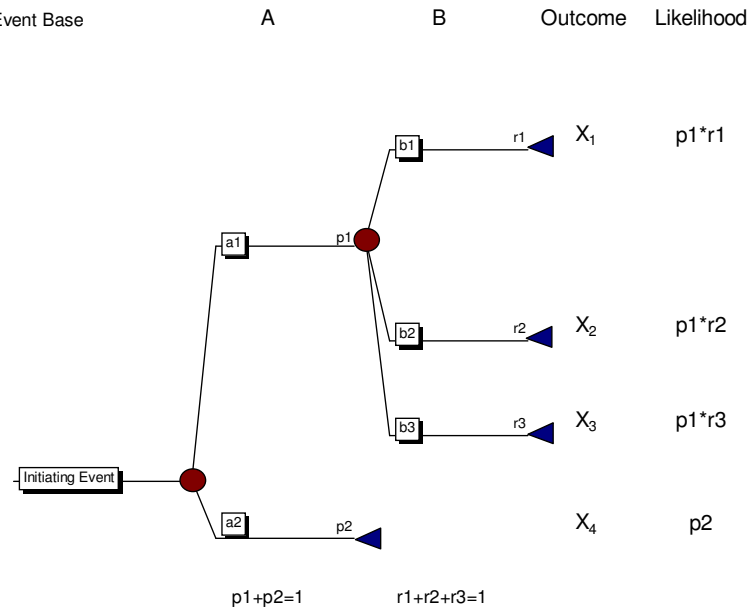


Figure 3 - Example of an Event Tree

The basic concepts and terms used in the discussion of event trees are summarized in Table 7. The basic events may correspond to elements of a physical process, human actions or responses to a question (Papazoglou, 1998: 170). Since the branches of the tree are exhaustive and represent the possible outcomes of each basic event, the paths are considered mutually exclusive; that is, there are no two paths that lead to the same outcome (Papazoglou, 1998:175).

Table 7 - Event Tree Terms & Definitions

Event Tree Element	Definitions	Example	Source Papazaglou, 1998
Basic Event (e_i)	Components wich decribe all possible things that can happen	A	170
Event Base (E)	Collection of events, whose outcomes completely describe the outcomes of a system	(A, B)	171
Joint Event (e)	Product of basic events; $e = e_1 * e_2$	A * B	171
Outcome of Event (ω)	Result of a basic event	X4	170
Outcome Space (W)	The distinct and finite set of all possible outcomes	W={X1,X2, X3, X4}	170
Partition of Outcome Space	The set of disjoint subsets which represent W	W=P1(W) U P2(W)	171
Path of Event Tree	Collection of branchs corresponding to an outcome	(a1, b1) or a2	175

The terms in Table 7 provide the foundation needed to discus methods for reducing the outcome space into collections of similar outcomes instead of all possible outcomes (Papazoglou, 1998: 169-170).

Two topics important to the reduction of the outcome space are *cylinder sets* and *cylinder paths*.

> Definition 3: Let E be an *event base* with N basic events, e_i (i=1,2,…,N) with corresponding *event-outcome spaces* W_i (i=1,2,…N) and the outcome space W. Also, let W_i be partitioned in the following manner $W_i = P_1(W_i) \bigcup P_2(W_i) \bigcup ... \bigcup P_j(W_i)$.
> Then a *Cylinder Set* is: $C = \{\omega\} = \{\omega_1 \in P_i(W_1) \wedge \omega_2 \in P_j(W_2) \wedge ... \wedge \omega_N \in P_k(W_N)\}$; were $\wedge$ is the conjunction operator (Papazoglou, 1998: 172).

A cylinder set represents a "generalized outcome" of a joint event, *e* (Papazoglou, 1998: 172). Papazoglou also explains that since a cylinder set contains distinct outcomes of the

outcome space, *W*, which are contained in respective subsets, cylinder sets are mutually exclusive (1998:172).

> *Definition 4:* A *cylinder path* is a subset of paths corresponding to a cylinder set of the outcome space (Papazoglou, 1998: 175).

A cylinder path represents a "generalized outcome" of basic events, which is restricted by the subsets of the corresponding outcome spaces (Papazoglou, 1998: 176). Thus an outcome space of a joint event is partitioned into subsets creating mutually exclusive cylinder sets. The paths corresponding to the cylinder set can then be reduced to the cylinder paths.

Since the likelihoods of events are expressed as probabilities, the cylinder sets and paths provide the opportunity to utilize probabilistic properties. Specifically, for an outcome space, $P[W]=1$. In addition, since the paths are mutually exclusive, then $P[A \cup B] = P[A] + P[B]$. Thus, for a cylinder set $P[C_i] = \sum_j P[\omega_j]; \ \forall \omega_j \in C_i$.

Applying the concept of cylinder sets and cylinder paths to Figure 3, the following assumptions are made: for basic event A, $p_1 + p_2 = 1$ and for basic event B, $r_1 + r_2 + r_3 = 1$. Let cylinder set, $C_1 = \{X_1, X_2\}$ be a success (S) and $C_2 = \{X_3, X_4\}$ be a failure (F). The new event tree is then depicted in Figure 4 .

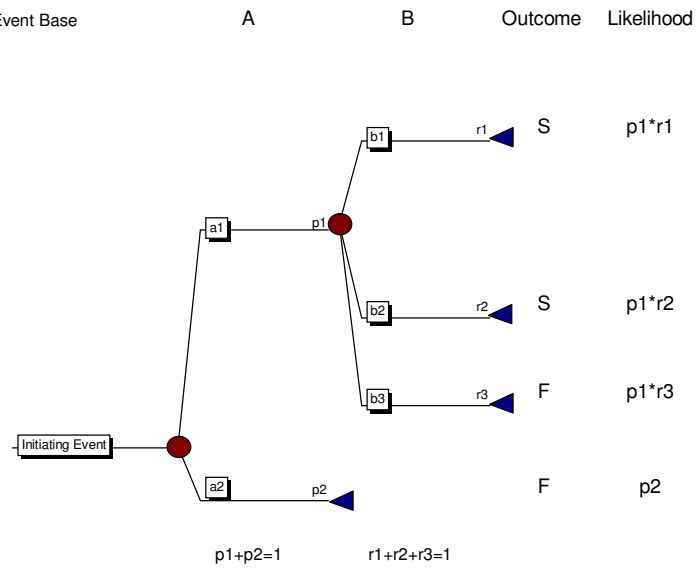


Figure 4 - Reduced Outcome Space Event Tree

2.4.3 Risk Importance Measures

Risk importance measures provide a quantitative means to determine a component's impact on the reliability of the overall system (van der Boorst and Schoonakker, 2001: 241). The two main categories of measures include: 1) a component's contribution to maintaining the current system reliability, and 2) the improvement to the system reliability given the improvement of a specific component.

Table 8 provides definitions and calculations from the literature for the importance measures were $x_i = 0$ indicates a no failure and $x_i = 1$ indicates a failure.

Table 8 - Risk Importance Measures

Importance Measures	Definition	Equation	Source
Risk Reduciton	Difference between current system reliability and the reliability when component *i* is completely reliable	$RR_i = P(F) - P(F \mid x_i = 0)$	Vesely *et al*., 1983:5
Risk Reduciton Worth	Ratio of current system reliability and reliability with a perfect component *i*	$RRW_i = \frac{P(F)}{P(F \mid x_i = 0)}$	Pottonen, 2005:91
Fussell-Vesely	Identifies the component most likely to cause a system failure	$FV_i = \frac{P(F) - P(F \mid x_i = 0)}{P(F)}$	Vesely *et al*., 1983:7
Risk Achievement	Difference between current system reliability and the reliability when component *i* is completely unreliable	$RA_i = P(F \mid x_i = 1) - P(F)$	Vesely *et al*., 1983:3
Risk Achievement Worth	Ratio of system reliability with an imperfect component *i* and current system reliability	$RAW_i = \frac{P(F \mid x_i = 1)}{P(F)}$	Pottonen, 2005:91
Birbaum's Measure	Reliability importance of component *i*; independent of current state	$BI_i = P(F \mid x_i = 1) - P(F \mid x_i = 1)$	van der Borst and Schoonakker, 2001:242

For all measures, $P(F)$ is the probability of system failure under the current reliability of components, $P(F \mid x_i = 0)$ is the conditional probability of system failure, given component *i* will never fail and $P(F \mid x_i = 1)$ is the conditional probability of system failure given component *i* will always fail.

While these measures prove useful individually, it is suggested that the combination of measures provided the best insight into the contributions of individual components and the overall system reliability, as different measure provide different information (Vesely *et al.*, 1983: 1; van der Boorst and Schoonakker, 2001: 242). Caution should be exercised in choosing which measure to use, as some measures are inter-related; as seen in Equations (2.13) - (2.15).

$$FV = \frac{RR}{P(F)} \tag{2.13}$$

$$RRW = \frac{1}{1 - FV} \tag{2.14}$$

$$RAW = \frac{RA}{P(F)} + 1 \tag{2.15}$$

2.5 Preference Functions

Preference functions provide a quantitative means to attribute a score to a set of alternatives. Through this research, the alternatives of interest correspond to the members of the network. A preference function separates the measure into parts, determines a value of the parts and then integrates the parts (Keeney, 1992:132-133).

2.5.1 Additive Linear Preference Model

Though the proxies for social importance, risk importance and spatial importance, are likely not mutually exclusive, Stewart suggests an additive linear preference model is still appropriate for use (1991:19). The linear preference functions are comprised of two components: the criticality proxies and weights. While normally calculated via single-dimensional value functions, the proxies used in this research are found by other methods. Finally, weights are needed to attribute a relative importance between the values of the linear model. The resulting function is represented in Equation (2.16) (von Winderfeldt and Edwards, 1986: 276).

$$v(x) = \sum_i w_i v_i \tag{2.16}$$

The weights needed, can be determined via a number of methods. These methods are categorized by Numerical Estimation Methods and Indifference Methods (von Winderfeldt and Edwards, 1986: 277-278). The following sections provide the explanation calculation for various weighting methods.

2.5.2 Weighting Techniques

Various weighting schemes are available to be employed, depending on the resources available and the urgency of the results. Some methods involve varied amounts

of inputs from Subject Matter Experts (SME), while others can be developed via available data. The weighting techniques in which SME inputs are necessary will focus on rating and rank methods, while those using data will incorporate proportions.

SMEs are a valuable asset for providing insight, however a drawback to using SME information lies in the differences of opinion between different SMEs. Methods of weight rating which are heavily reliant on SME inputs and thus specific to that SME are direct rating, Simple Multiattribute Rating Technique (SMART) and the Max100 point allocation. It is argued by Bottomley *et al.* that direct rating techniques produce linearly related weights where as point allocation methods produce non-linearly related weights (2000: 553).

One alternative for calculating weights is direct rating. A SME ranks the options, giving the lowest a score of zero and the highest a score of 100. The options in between are assigned a value between zero and 100. A consistency check is done comparing all options pairwise to determine the final weights, which are then normalized. von Winderfeldt and Edwards highlight that direct rating is seldom used, but offer the dispersion of a total of 100 points across the attributes as an alternative method (1986: 274-275). An easier version of this method requires only that a SME allocate a total of 100 points among all options relative to the importance placed on each option.

The swing weights presented by Kirkwood are adapted from Edward's SMART (1997: 53). This procedure requires significant inputs from the SME, as the relative importance for each attribute must be determined. The procedure is outlined in the following four steps (Kirkwood: 1997: 70):

1. Rank the attributes from least important to most.

2. Assigning the lowest importance attribute a value *k*, scale the remaining attributes as a multiple of the lowest.

3. Sum the values, set equal to one and solve for *k*.

4. The value of *k* should then be multiplied by the scaling numbers to obtain the weight of each attribute.

Max100 is a method of ratio estimation weighting, which relies on the SMEs perception of attribute importance relative to that considered most important. The Max100 method applies similar techniques to those used in SMARTS. The procedure is outlined by Bottomley and Doyle (2001: 555):

1. The attributes are ranked according to importance.
2. A value of 100 is assigned to the attribute considered most important.
3. The remaining attributes are then given a value between zero and 99, as a relative importance to the most important attribute.
4. Score are normalized.

Bottomley and Doyle offer the observation that the consistency of alternative ranking based on the results from the Max100 weighting in testing displayed fewer rank reversals (2001: 559).

Two weighting methods requiring less SME inputs involve only an ordinal ranking of attributes. The most important attribute is assigned one, such that $R_1 = 1$, $R_2 = 2$,..., $R_n = n$. The Rank Reciprocal (RR) rule is shown in Equation (2.17) (von Winderfeldt and Edwards, 1986: 284).

$$w_i = \frac{1/R_i}{\sum_j \left(1/R_j\right)} \tag{2.17}$$

Another rank based weighting method is the Rank Sum (RS), seen in Equation (2.18) (von Winderfeldt and Edwards, 1986: 284):

$$w_i = \frac{(n+1-R_i)}{\sum_{i=1}^{n} R_i} \tag{2.18}$$

For the simple case of three and six attributes, as seen in this research, Figure 5 and Figure 6 depicts the calculated weights. The Rank Sum weights appear linear, while the Rank Reciprocal weights are piece-wise linear, giving more importance to the higher ranked attributes. A choice between these two methods should reflect the perceived importance of the attributes from the SME.

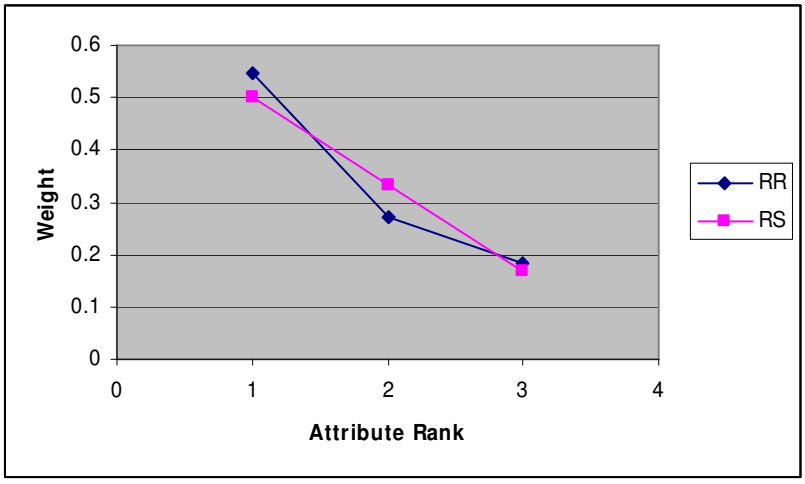


Figure 5 - 3 Attribute Comparison of RR and RS

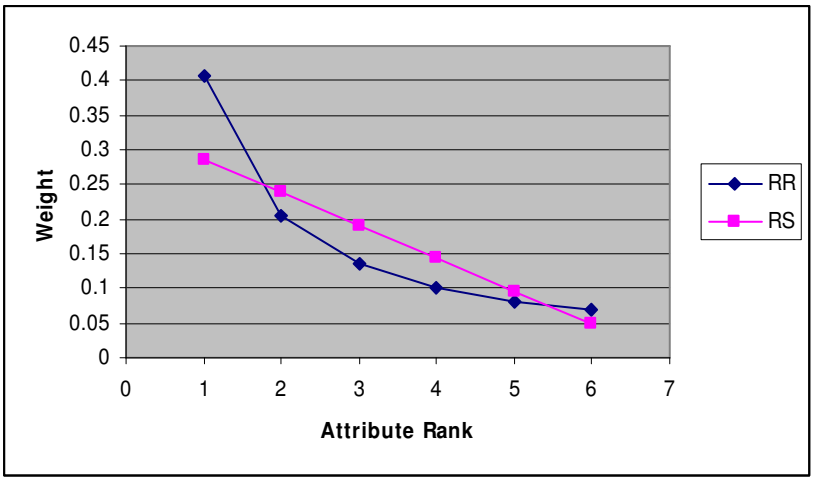


Figure 6 - 6 Attribute Comparison of RR and RS

Finally, there is a weighting system that does not rely on the inputs of a SME, but provides a calculation based on a proportion of data. This method of weighting was introduced in Hamill's layered view of Social Networks. The weighting measure for a specific layer is determined by the proportion of data contained in a specific layer to the total amount of data. The potential problems with this method arise from the accessibility to information; some groups, affiliations, and so forth are easier to develop information. The proportional weight is given in Equation (2.19) (Hamill, 2006: 215):

$$w_l = \frac{E_l}{E_L} \tag{2.19}$$

2.6 Conclusion

This section incorporated a variety of Operations Research techniques as well as social sciences and mathematics. Topics focused specifically on organized crime and terrorist groups, the uses of SNA measures and advancements, risk analysis techniques and weighted preference functions. The material covered underpins the methods and theories used throughout the remainder of this research.

3 Methodology

3.1 Introduction

The aim of this research is to determine how critical an individual is to a network and its operations. Ultimately, the goal of this criticality measure is to identify the individual or individuals, who if influenced or removed from the network of interest, would be most likely to adversely impact or temporarily halt undesired operations.

The contributions of Social Network Analysis (SNA) and Social Influence Network (SIN) theory (Katz, 1953; Taylor, 1969; Granovetter, 1973, 1983; Freeman, 1979; Bonacich, 1987; Sade, 1989; Stephenson and Zelen, 1989; Bonacich, *et. al.,* 2004, Newman, 2004), along with the advancements of the meta-matrix components (Carley and Krackhardt, 1999, Carley *et al.*, 2000) provide a framework and the tools needed to determine an individuals importance across the many layers of social and operational connections between group members.

The criticality measure is comprised of three components: 1) the individual's social connections, 2) the skill and/or resource connections needed for successful operations, and 3) their location or proximity to important individuals or events over an operational period. The information needed for each of these factors is summarized in Table 9.

Table 9 - Information Required for Analysis

Social Importance	Operational Importance	Location Importance
▪ Connections between group members based on each affiliation of interest ▪ Weights for the importance of each type of affiliation	▪ Reliability/Availability/ Accessibility of each skill and material needed to conduct an operation ▪ Skills/Materials each member possess or has accessible to them ▪ Tasks each member is capable of completing	▪ Location of members based on time periods of interest

Figure 7 provides a review of the components of the proposed analysis method.

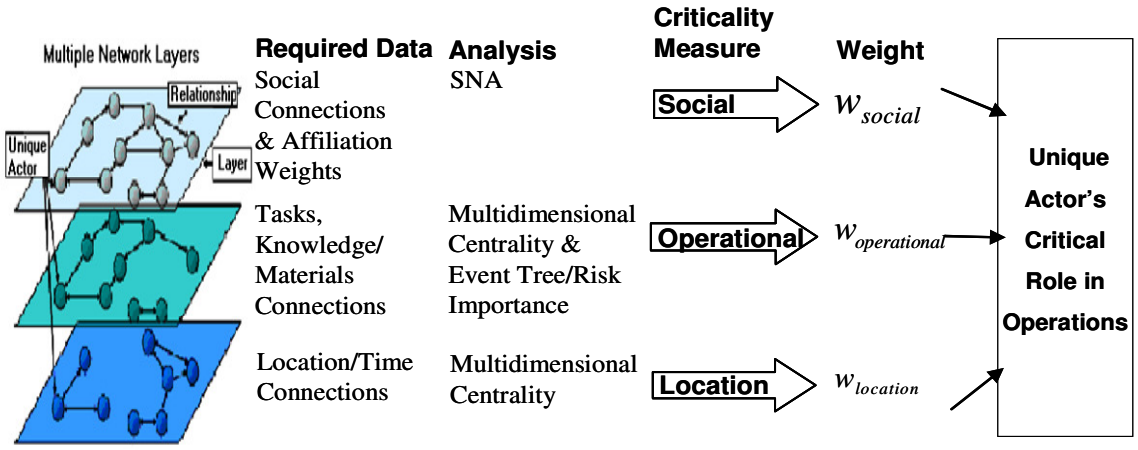


Figure 7 - Analysis Process Diagram

The following sections of this chapter explain in detail the approach for calculating the criticality of each of the three components.

An example network, with social, operational, and location information is provided only as a means to demonstrate the concepts throughout Chapter 3. The example is notional and has no affiliations to any *real-world* organization.

3.2 Social Importance

The multitude of Social Network Centrality and Social Influence measures provide a number of options to analysts to analyze the importance of an individual based on his or her position in the network. The fact that most clandestine networks use some Operational Security (OPSEC) practices, as demonstrated in the *al-Qaeda Training Manual*, the boundaries of membership are not know with certainty (Post, 2005). This leads to a limitation in the types of centrality measures that are considered appropriate or "stable", especially in the face of imperfect data (Constenbader and Valente, 2003). Other important considerations for centrality measures of networks rely on the

directedness of relationship, the probable strength of the relationship, the number of intermediaries between members and so forth.

The concepts of formal and informal networks are a mechanism for identifying the nature of the relationship between members. Tichy *et al*. recognizes this as "transactional content" were relationships contain one of the following four types: "1) exchange of affect (liking, friendship), 2) exchange of influence, 3) exchange of information and 4) exchange of goods or services" (1979: 508). Since relationships can exist in any or all of the capacities above, decomposing the network into the appropriate formal and informal networks provides insight into the strength of member connections as the combination of multiple affiliations.

Through the compilation and analysis of open source information available for known and suspected terrorists, Sageman identifies sets of network affiliations. These social affiliations include: *acquaintance, friendship, kinship (nuclear family and relatives), discipleship and worship* (2004: 107-120). Carley *et al.* suggest co-worker and group members as examples of additional affiliations which could be incorporated into an analysis (2006: 257). Figure 8 represents the composite and layered connections of a five member cell. To determine an individual's importance to the social network, various methods are investigated.

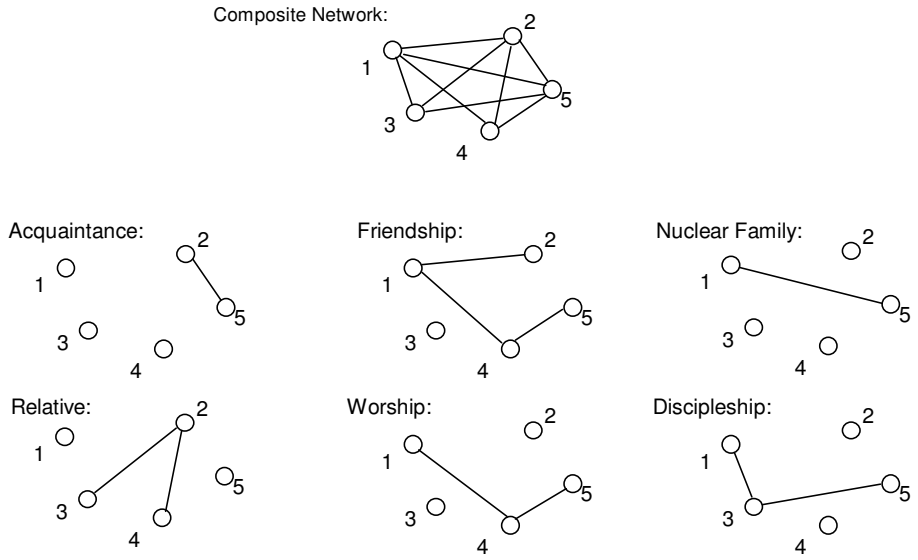


Figure 8 - Five member cell: Composite & Layered Connections

3.2.1 Layer Weighting

The amount of influence a person has on another's life is dependent on the nature of the relationship between the two people (Granovetter, 1973: 1361). For this reason, an importance level must be found for the affiliation types in the network. When possible, Subject Matter Experts (SME), familiar with knowledge of a group's culture, should be consulted for inputs. A caution with SME inputs stems from the importance placed on relationships in different cultural regions. This research investigates multiple methods for determining weights of affiliation layers.

Swing Weights are the theoretically most preferred form of weighting, but are highly reliant on SME inputs. A benefit of swing weights emerge from the relative importance place on one attribute over another by the SME (von Winderfeldt and Edwards, 1986: 298). A drawback of swing weights in the context of Social Networks arises from the loss of generality due to the difference in cultural values; this requires additional SME inputs to account for groups in different cultures. The swing weight,

based on the Simple Multiattribute Rating Technique in Section 2.5.2, calculations are summarized in Equation (3.1) and Equation (3.2) (Kirkwood, 1997: 70).

$$\begin{aligned} &\text{Let : } w_1 = k,\ w_2 = \alpha k, \ldots,\ w_n = \alpha_{n-1} k \\ &\text{were } \sum_{i=1}^{n} w_i = 1 \end{aligned} \tag{3.1}$$

$$\text{Then, } k = \frac{1}{1 + \sum_{j=1}^{n-1} \alpha_j} \tag{3.2}$$

A simple ordinal ranking from a SME, while less desirable, provides a basis for the importance of relationships. Layers should be ranked from most important to least important. Of the von Winderfeldt and Edwards measures introduced in Section 2.5.2, the rank reciprocal rule is used due to the increased importance placed in the top ranking affiliation types. Equation (3.3) represents the Rank Reciprocal Rule (1986: 284):

$$w_i = \frac{1/R_i}{\sum_j \left(1/R_j\right)} \tag{3.3}$$

Hamill introduces a weighting scheme that when applied, would consider the proportion of arcs contain on a specific layer to the total number of arcs in the network across all layers (2006: 215). While this method is not dependant on a SME with cultural or regional knowledge of the group, it is not without pitfalls; intelligence analysts often know or are able to develop more information about some affiliations than others between group members. As a result, layers which are actually less influential may be given a higher weight due to the density of the information collected. The weights w_l for a specific layer is the proportion of E_l, the number of arcs contained in layer l and E_L, the sum of all arcs in the network as given by Equation (3.4) (Hamill, 2006: 215):

$$w_l = \frac{E_l}{E_L} \tag{3.4}$$

Applying this method of weighting to the layers in Figure 8, the following weights were calculated: Acquaintance (.09), Friendship (.27), Nuclear Family (.09), Relative (.18), Worship (.18) and Discipleship (.18).

Weights for a network are important to determining which relationships carry more influence in enhancing a person's importance with the network, but there is no consistent manner in which these weights are chosen. If a SME is available and able to give inputs for swing weights, this is preferred. If time, location or access does not allow for swing weighting, the "100 balls" technique, with its shortfalls, may be considered. If the model has the potential to be used for groups across differing cultures, the rank reciprocal rule may be more robust. If an analyst is not comfortable with the results of the layer proportions, considering all weights equal is yet another option for an analyst. Finally, a mix of techniques may be applied as time and importance of the analysis and modeling allows. The analytic situation will dictate which method is most appropriate, although time and resources permitting, swing weighting is preferred.

3.2.2 Centrality Measures

The appropriateness of centrality measure use is dependent on the structure of the network and the information desired. As detailed in Section 2.3.1, the centrality methods covered are used in the SNA community, which Carley contends are appropriate for covert networks when taken in combination with the dynamic relationships involving tasks and resources (2003: 3). Due to the secretive nature of the terror organizations and the sparseness of the connections, some things are known or may be assumed about the

structure of the group. The individual's importance may pertain to their position as an intermediary between members (betweenness centrality), their role in perpetuating information through the network (information centrality), or the prestige of a person base on those they are connected to (eigenvector centrality) (Wasserman and Faust, 1994: 188-198 and Bonacich *et al*, 2004: 192). All information about the group and the desired information about the members is evaluated through the remainder of this section.

Since betweenness looks at shortest paths were a specific member is on the path between two other members, there may be promise in determining this value. The key advantage of identifying this individual would be apparent in their removal from the network, as members would then be disconnected and the paths to propagate a message would be longer (Borgatti, 2005: 60). In a study by Borgatti *et al.* were nodes and arcs were added and removed from random graphs, betweenness centrality appeared slightly less sensitive to possible imperfect data than degree, closeness and eigenvector centralities (2006: 134).

Similar to betweenness, information centrality identifies members of a network who lie on the path between two other members (Wasserman and Faust, 1994: 193). The strength of information centrality is attributed to the consideration of all paths connecting two members, not just the shortest path (Stephenson and Zelen, 1989: 3). Hamill's research identifies a problem with inconsistencies in calculation methods offered by Stephenson and Zelen, but suggests that calculations done strictly by Stephenson and Zelen's definition removes the potential for error (2006: 304-308). This error is especially troubling in light of the potential for imperfect data in large clandestine groups, as the need for all paths between members propagates the potential for error.

Eigenvector centrality uniquely considers a member's importance based on the importance of the individuals to whom the member is connected (Bonacich *et al.*, 2004: 192). In other words, you are only as important as the people you know. In a comparison of multiple centrality measures, eigenvector centrality was favored in cases were "network data is incomplete" (Constenbader and Valente, 2003: 305); given the secrecy of clandestine groups and knowledge that data is likely incomplete, eigenvector centrality is a suitable choice. Stephenson and Zelen argue a limitation to this method is caused by the inability to consider "multiple paths" between members (1989:4). Advancements to Eigenvector Centrality adapt the measure for use with weighted graphs (Newman, 2004).

3.2.3 Combining Layers

An initial method for combining multiple layers of social networks, introduced by Clark, combines an individual's characteristics and centrality measure (2005). Since this research is concerned with the centrality, the personal characteristics will not be included. Clark's calculations included the use of Information Centrality (described in Section 2.3.1) for each affiliation layer, then used an additive function with equal weighting to give a total Centrality Measure. Equation (3.5) represents the weighted centrality used by Clark, where w_i represents the weight associated with the *ith* affiliation layer and I_i the vector of centrality scores for all members for the *ith* affiliation layer (2005: 3-25):

$$W = w_1 I_1 + w_2 I_2 + \ldots w_n I_n$$
$$\sum_{1}^{n} w_i = 1 \tag{3.5}$$

The second method, introduced by Hamill, calculates the information centrality of members based on valued relations (2006: 201). Adjacency matrices, as used by Clark,

fail to account for the relative strength of relationships within the network. Hamill incorporates an additive value of dynamic weights to determine the relationship strength, as indicated by Equation (3.6):

$$S_{ij} = \sum_{l=1}^{n} w_l x_{ijl}$$

$$\text{were: } w_l = \text{ weight of layer } l \tag{3.6}$$

$$x_{ijl} = \begin{cases} 1; \text{ if arc exists between } i \text{ and } j \\ 0; \text{ if no arc exists} \end{cases}$$

The result of this method, applied to the layered connections of Figure 8, using the layer proportional weighting produces the following weighted graph (Figure 9):

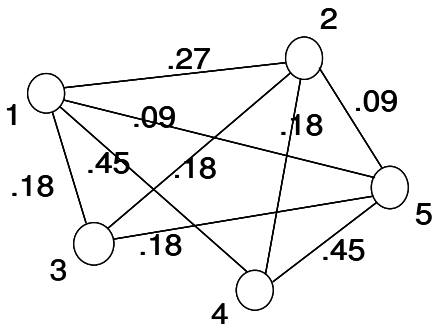


Figure 9 - Five Member Cell -Weighted Graph

3.2.4 Section Summary

This section reviews methods for determining an individual's social importance. The understanding that relationships exist based on different types of affiliations, allows analysts to investigate the nature of the group members based on those layers. The influence a person has on others depends on the type of affiliation the two members share, this leads to the need to prioritize the affiliations via weights. Weights calculated via SME inputs are most desired, but alternative methods may be necessary. The centrality measures provide a means to determine the power or influence a member has within the network. Finally, the two components must be merged; Clark and Hamill

provide similar approaches (Clark, 2005; Hamill, 2006). The Social Importance acts as only one element to a member importance, the two remaining elements are introduced in the following sections.

3.3 Operational Importance

In addition to the social importance a member holds within a clandestine network, consideration must also be given to the operational value of the members. Viewing these operations from a project management perspective, management of the group's *resources* is essential to any project's completion or in the case of terror groups, successful attacks (Shtub *et al.*, 2005: 457). *Resources* in this context can refer to personnel, expertise or materials; each group's *resources* will depend on their tactics. The availability or reliability of these *resources* will impact the project completion or operational success.

The criticality of a task can be attributed to precedence of the tasks, the availability of personnel to complete, especially those needing a specific expertise, and the availability or reliability of the resources used in completion of the task. The first measure used in this section represents the importance of each task. The following section measures the criticality of the skills/expertise and materials to the task's completion. Finally, the factors are combined to give an operational score for each member of the group.

3.3.1 Task Importance

Task completion is essential to a group's continued operational success, especially in the case of conducting attacks. Bonacich *et al.*'s multidimensional centrality applied to a member/task incidence matrix, as shown in Table 10 , provides a measure for task

centrality based on the number of personnel *capable* or *available* to complete the task (2004). Using the incidence matrix as *E*, the calculation includes the eigenvector associated with the largest eigenvalue of E^TE (Bonacich *et al.*, 2004: 195). This, however, conflicts with what is needed, since the tasks with fewer people capable or available has a greater potential for being incomplete, should the members become incapacitated or unavailable. Hence, the reciprocal of the values from the eigenvector is used, to give tasks with fewer members a higher value. Normalization of the reciprocal values provides a proxy measure of importance relative to the other tasks.

Table 10 - Member/Task Incidence Matrix

	task1	task2	task3
member 1	1	0	1
member 2	0	1	0
member 3	1	0	0
member 4	1	0	1
member 5	0	0	1

An issue that arises with some data, for example that contained in Table 10, results from a value of 0 for task2. Since the reciprocal can not be taken, some small epsilon (i.e. 0.01 or 0.001) should be used in the place of the 0. This epsilon method, however places an unrealistic portion of importance on the task. Hence, in some situations, an alternative method may be needed.

An alternative to the eigenvector centrality calculation is the proportional weighting suggested by Hamill, as explain in Section 2.5.2 (2006; 215). This method would account for members capable of completing a specific task, as a proportion of the sum of members capable across all tasks. A comparison of the two methods is provided in Table 11.

Table 11 - Comparison of Eigenvector Centrality & Proportional Task Scores

	eigenvector centrality	modified eigenvector centrality	**normalized, reciprocal of eigenvector centrality**	proportional weight	**normalized, reciprocal of proportional weight**
Task1	0.71	0.71	**0.01**	0.43	**0.20**
Task2	0.00	0.01	**0.97**	0.14	**0.60**
Task3	0.71	0.71	**0.01**	0.43	**0.20**

A potential argument concerning this method for determining task importance is likely to come from discussion around tasks were few members are capable or available. The case could be that the task is simplistic and needs very few members to support. However, if this is the case, more members should be available or capable of completing the task. Thus it is assumed that the member/task incidence matrix represents the members capable or available to complete the specific task, not the number of people needed or assigned to the task. If this assumption holds, then all other things being equal, tasks with few members will more likely be incomplete, due to non-redundancy, should the individual(s) be removed from the network or influenced not to complete the task.

3.3.2 Event Tree/Reliability

System or operational analysis is a specific application of probabilistic risk analysis (PRA) or reliability analysis (Høyland and Rausand, 1994: 9). By viewing an organization's operations as a system with components, which may or may not be reliable at a given time, PRA can be applied. The components used in evaluating the system represent the skills and/or materials used by the members to conduct operations. From the terror organization's view, an operation or attack is either successful or unsuccessful; numbers of casualties are not necessarily an indicator of success, since a target could potentially be part of the adversary's infrastructure. Thus the outcome, or *consequence*, represents either a success or failure. This section focuses on the use of *Event Trees* to

determine the risk to the terrorist organization of an operation or attack being unsuccessful. The following section provides methods for calculating probabilities, followed by measures of importance or criticality for the skills and/or materials needed to ensure operational success.

In an effort to move away from the use of imprecise estimates of probabilities in this risk analysis, numerical probabilities are used in the event tree. Though much of the specific data pertaining to the availability or reliability of resources of a terrorist organization is likely classified, statistical methods exist to calculate probabilities. One possibility is found in Haimes (2004). He suggests triangular distributions as a method which requires SME inputs. Triangular Distributions require three values, the most likely value (c), best-case value (b) and worst-case value (a), which are combine to provide a probability density function with an expected value, given by Equation (3.7) (2004; 156-158):

$$E[X] = \frac{a+b+c}{3} \tag{3.7}$$

A method solely based on available data is frequency counts; the frequency of a specific outcome is taken a proportion of the total number of outcomes. For example, if 50 similar events are observed and outcome A occurred 13 times, then the likelihood of outcome A could be estimated as 13/50 or 26%. Other such approaches exist and should be applied to estimating probabilities where sufficient data exists (Haimes, 2004: 138).

Event Trees are one method used for observing and calculating probabilities associated with risk (Bedford and Cooke, 2001: 99). The risk triple, as covered in Section 2.4.1, $R = \langle S_i, L_i, X_i \rangle$ where S_i represents a risk scenario, L_i is the likelihood of the scenario and X_i is the outcome associated with the scenario (Kaplan and Garrick,

1981: 13), contains information about the specific risk associated with a component of the system/operation, likelihood and consequence of the event (Haimes, 2004: 92-93). Event Trees typically represent binary events (i.e. success/failure, available/unavailable, etc.), but the characteristics of a component, acting as an event in the tree, can represent any possibilities of interest (Papazoglou, 1998: 170). For example, a system's flow capacity at high, medium and low/none may be of more interest than a simple flow/no flow scenario. Event Trees are simply a modeling tool to aid the analysis of outcomes based on the logic and likelihood of "simpler events" (Papazoglou, 1998: 170).

Based on reports of attacks and the known tactics practiced by some groups, Suicide Bombings are an attack mechanism increasingly practiced by terrorist groups (Pape, 2003). This scenario is used here to illustrate the methodology of using event trees to evaluate the risks associated with such a simple operation. For the purpose of discussion, it will be assumed, there are three components to a suicide bombing scenario: a bomber, an explosive and a target (Pape, 2003: 345).

The likelihoods used in the section are merely to demonstrate the methodology; the likelihoods for these components in an actual operational scenario, would depend largely on the group's goals, tactics, quality of munitions and member composition. Actual likelihoods should be developed based on the historical patterns and knowledge of the ongoing operations of the terrorist group. The bomber selected for an operation carries a reliability; assume there is an 85% likelihood the bomber is willing to detonate the explosive device when they arrive at the target. There is also a reliability associated with the explosives; assume there is a 90% likelihood the munition will detonate at the target and only 10% likelihood it is defective or will pre-detonate, killing only terrorists in

preparation of the attack. Finally, surveillance is needed for a target to determine potential security risks and the time of maximal civilian or adversary proximity; assume the surveillance conducted for a target is 99% accurate for a given time period and only 1% inaccurate, making the target inaccessible. Figure 10 represents the event tree for the outlined notional scenario.

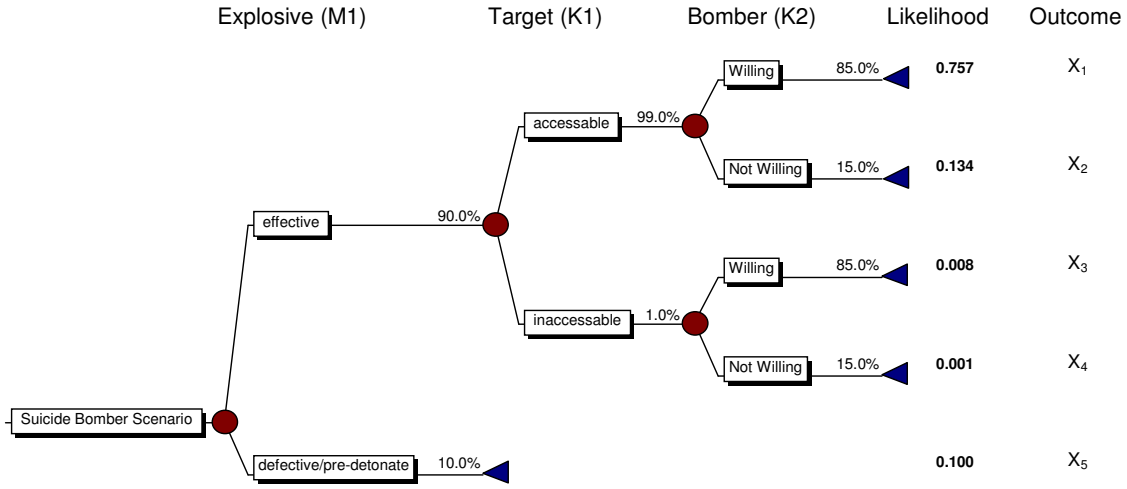


Figure 10- Event Tree Suicide Bombing Scenario

The event tree shows five possible outcomes $\{X_1, X_2, X_3, X_4, X_5\}$ with respective likelihoods of (0.767, 0.134, 0.008, 0.001, 0.100). The failure of any component will result in a mission failure, with the exception of the surveilled target, as the bomber would likely detonate in-place should a barrier or security interfere. According to Papazoglou, the outcome space can be partitioned into two mutually exclusive subsets, were Mission Success = $\{X_1, X_3\}$ and Mission Failure = $\{X_2, X_4, X_5\}$ (1998: 173). Since the partitioned outcome spaces have been constructed to be mutually exclusive, a probability for each is determined by Equations (3.8) (Papazoglou, 1998: 180):

$$P[MS] = \sum_i P[X_i]; \quad i = 1,3$$
$$P[MF] = \sum_j P[X_j]; \quad j = 2,4,5 \tag{3.8}$$

The result then indicates that the estimated probability of a Mission Success is 0.765 and the estimated probability of Mission Failure is 0.235. The intended use of event trees is for the reliability analysis of the components, thus risk importance measures are incorporated in the next section.

Since suicide attacks are not the only tactic exploited by terror groups, event trees for other types of attacks are included. Chapter 4 contains an example with an Improvised Explosive Device attack. Appendix A contains important components for other attacks including: Chemical, Biological, Radiation and Nuclear weapons.

3.3.3 Risk Importance Measures

The purpose of the Risk Importance Measure is to identify the risk associated with each component of the system or operation (van der Boorst and Schoonakker; 2001). This methodology aims to provide a relative measure of importance for the components which have the greatest potential to cause a mission failure. The Risk Importance Measures, introduced in Section 2.4.3, are intended to exhibit various aspects of a system's potential for risk and the risk contributing components. These measures focused on "risk reduction and risk achievement" (van der Boorst and Schoonakker, 2001: 241-242). The risk reduction measures quantify the improvement to a system if a component were perfect (Vesely *et al.*, 1983: 5). The risk achievement measures determine the risk should a component always fail (Vesely *et al.*, 1983: 3). A combination of the multiple measures provides an analyst with the best perspective of what is likely to increase or decrease the reliability of the system when the component reliabilities change (Vesely *et al.*, 1983: 1; van der Boorst and Schoonakker, 2001: 242).

The Risk Importance Measures considered for this methodology included a mix of risk reduction and risk achievement measures, as introduced in Section 2.4.3. Several of the measures are either directly or inversely related, therefore only those which are unrelated were considered (Vesely *et al.*, 1983; Høyland and Rausand, 1994, van der Boorst and Schoonakker, 2001; Pottonen, 2005). Due to the consideration for the proportion of improvement, this research will used the Fussell-Vesely measure, as it aids in the identification of the component most likely to cause system failure (Høyland and Rausand, 1994:203); shown in Equation (3.9) (van der Boorst and Schoonakker, 2001:242).

$$\text{Fussell-Vesely}: \quad FV(i) = \frac{P(MF) - P(MF \mid x_i = 0)}{P(MF)} \tag{3.9}$$

Another commonly used measure is the Risk Achievement Worth measure, which quantifies the impact a component has on the current level of system reliability (Pottonen, 2005: 92); shown in Equations (3.10) (van der Boorst and Schoonakker, 2001:242).

$$\text{Risk Achievement Worth}: \quad RAW(i) = \frac{P(MF \mid x_i = 1)}{P(MF)} \tag{3.10}$$

For both measures, $P(MF)$ is the probability of Mission Failure under the current reliability of components, $P(MF \mid x_i = 0)$ is the conditional probability of Mission Failure, given component *i* does not fail and $P(MF \mid x_i = 1)$ is the conditional probability that component *i* always fails.

To combine these two measures, each should be normalized, via the one-norm, to provide a relative importance, before the measures are averaged. The results for the Suicide Attack scenario used in the previous section are provided in Table 12.

Table 12 - Fussell-Vesely & RAW Measures Combined

Resource	FV	**Normalized FV**	RAW	**Normalized RAW**	**Average**
Explosive (M1)	0.36	**0.39**	4.26	**0.45**	0.42
Target (K1)	0.00	**0.00**	1.00	**0.11**	0.05
Bomber (K2)	0.57	**0.61**	4.26	**0.45**	0.53

The results in Table 12 show the Bomber willingness is the most important, while the Target availability is least. This confirms Pape's assertion that a willing Bomber is more likely to create the condition for a successful mission due to their flexibility (2003: 346).

3.3.4 Assigning Operational Value to Members

Ultimately, the operational importance value must be attributed to the group members. Under the assumption that the *resources* of a group are independent, an additive linear preference model easily combines the values (von Winderfeldt and Edwards, 1986: 276). Using the member/task, member/knowledge and member/materials incidence matrices, the overall operational criticality of a member can be assigned as presented in Equation(3.11) .

$$[M/T](TaskScores)+[M/K](KnowledgeScores)+[M/Mat](MaterialsScores) \quad (3.11)$$

[M/*i*] represents the Incident matrices associate with Task, Knowledge and Materials. (Scores) correspond to the vector of measures calculated for the Tasks, Skills/Knowledge or Materials importance. The scores for the members should then be normalized across the group to provide a relative value of importance for each member within the operational context.

3.3.5 Section Summary

The operational component to groups can be drastically different based on the group's relational dynamics, their goal and the tactics they implore. For this reason, a

variety of Operation Research techniques are needed to model the various aspects contributing to the operational success of a group. Tasks criticality and materials and skill/knowledge importance were those considered in this research. The eigenvector centrality accounts for the capability of members for across multiple tasks simultaneously, but creates the potential for error. The proportion of tasks method reduces the potential for error, making it less likely to place too much importance on any specific task unless warranted by a small number of available members. Event trees provide a means to calculate the probability a mission will succeed or fail, base on the reliability of the components (materials/skills). The probabilities are then used to evaluate the contribution of the components to a mission failure through the Fussell-Vesely and Risk Achievement Worth measures. Finally, all of the *resource* importance values are summed and normalized across the group, allowing an analyst to determine the member with the greatest operational criticality. It should be noted that since the probabilities for such events incorporate human actions, the precision associated with systems engineering reliability analysis is unlikely. This method, even with a level of imprecision, provides analysts a means to gain insight into terrorist attacks and operations.

3.4 Time and Location

To disrupt a network, time and location are two essential pieces of information. The movement of members provides insight into the locations for safe houses, meeting locations, weapons caches, and other such facilities. Locations can also provide information about event planning. The presence of personnel at a special training facility may indicate the need for improved skills to advance attack tactics. Timing and location

information near potential targets could provide insight into the groups' intent. The following section develops a method to quantify the potential importance of group member presence at locations during specific time periods.

The first approach for determining members' temporal and spatial criticality, comes from inputs of SME. A SME familiar with the group and its operations can provide invaluable insight into the importance of member location. These locations could be tied to training, meetings, materials movement, targets, or other operational factors. The value for a member whose location is unknown should also be obtained from the SME, if possible. The weighting of location importance can be found via swing weight or ranking, as introduced in Section 2.5.2.

When SMEs are unavailable, an importance value can be attributed to members based on their location over a given period or at different locations through several time periods. Bonacich *et al.*'s multidimensional centrality, discussed in Section 2.3.2, provides the mechanism to allow for social connections to be time and/or location dependent (2004). To achieve this, a member/connections (node-arc) incidence matrix is needed. The connections are represented in the rows of the matrix and the members make up the columns. This matrix is then augmented with the locations and/or time periods of interest and used to indicate the time or location a specific a connection occurred; resulting in $E = \left[M \middle| L \right]$; where $M = Member\ Incidence$, and $L = Location\ Incidence$ (Bonacich *et al.*, 2004: 201). This augmented matrix accounts for who was meeting whom and when and where they met. The calculation provides a measure for the location or temporal importance for connections or presence based on the importance of the members present at that location or during that time period.

This method does not account for certain occurrences that may also be of interest, such as an individual who appears at a location, but is not know to have met with other members or when a member's location is unknown for a specific period. Since leaving these individuals unaccounted for will produce a value of zero for their time and location criticality, a modification must be made. If a dummy node is added to represent a connection, the member's presence at a location can be accounted for. A dummy connection and location (i.e. location unknown) must be added when a member's location is unknown. The addition of the dummy connections and locations will increase the dimensionality of the matrix, especially for large networks.

Figure 11 represents the five member cell used in Section 3.3.1. The connections of members are considered at two separate locations over the same period of time (i.e. a week or month).

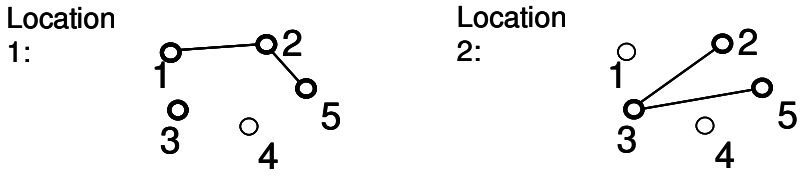


Figure 11 - Five Member Multi-dimension Graph

The bold nodes represent members who appeared at the location during a period of time. The arcs connecting members represent known meetings or connections at the specified location. Table 13 represents the node-arc incidence matrix, as proposed by Bonacich *et al.* (2004: 191).

Table 13 - Member & Location/Connections Incidence Matrix

	Member1	Member2	Member3	Member4	Member5	Location1	Location2
(1-2)	1	1	0	0	0	1	0
(2-5)	0	1	0	0	1	1	0
(2-3)	0	1	1	0	0	0	1
(3-5)	0	0	1	0	1	0	1

However, notice Member 3 was known to be at Location 1, but is unaccounted for in the incidence matrix. In addition, Member 4 does not appear in either location and would be give a value of 0; the fact that a member is unaccounted for may be of great significance. Unless a SME is able to provide an approximation for the significance of a member's presence being unknown, a proxy value greater than 0 should be calculated instead. Table 14 represents the proposed modified incidence matrix.

Table 14 - Modified Member & Location/Connection Incidence Matrix

	Member1	Member2	Member3	Member4	Member5	connection place holder	Location1	Location2	Loc Unk
(1-2)	1	1	0	0	0	0	1	0	0
(2-5)	0	1	0	0	1	0	1	0	0
3	0	0	1	0	0	1	1	0	0
(2-3)	0	1	1	0	0	0	0	1	0
(3-5)	0	0	1	0	1	0	0	1	0
4	0	0	0	1	0	1	0	0	1

The results of eigenvector centrality, as applied to the data in Table 13 and Table 14, are provided in Table 15. For the data in Table 13, the importance of Location 1 and Location 2 is equal. However, the data in Table 14 shows Location 1 as scoring higher, since more members were present at Location 1. This also imputes a value for the member whose location was unknown; while the number is small in this example, this will not always be the case.

Table 15 - Comparison of Location Importance

	eigenvector centrality of Incidence Matrix	**normalized eigenvector centrality of Incidence Matrix**	eigenvector centrality of Modified Incidence Matrix	**normalized eigenvector centrality of Modified Incidence Matrix**
Location1	0.39	**0.50**	0.48	**0.57**
Location2	0.39	**0.50**	0.33	**0.39**
Loc Unk	-	**-**	0.03	**0.04**

An extension to this method would be to allow the connections to carry the weights, as calculated by Hamill's method in Section 3.2.3. The five member cell

weighted graph produced the modified incidence matrix as displayed in Table 16. The normalized eigenvector centrality of the connections and locations, determines the location values as follows: Location 1 (.69), Location 2 (.06) and Location Unknown (.25). The location criticality value would then be added for each member across both locations and time periods. The member location values must be normalized via the one norm to provide the relative location importance of each member.

Table 16 - Modified Incidence Matrix Based on Weighted Graph

	Member1	Member2	Member3	Member4	Member5	connection place holder	Location1	Location2	Loc Unk
(1-2)	0.27	0.27	0	0	0	0	1	0	0
(2-5)	0	0.09	0	0	0.09	0	1	0	0
3	0	0	1	0	0	1	1	0	0
(2-3)	0	0.18	0.18	0	0	0	0	1	0
(3-5)	0	0	0.18	0	0.18	0	0	1	0
4	0	0	0	1	0	1	0	0	1

SME inputs for location are always preferred, as a SME will have the best understanding of the importance locations and time will have on the group's activities. Short of being able to get such information, the eigenvector centrality of the relationship matrix augmented provides a reasonable alternative. Since the approach can be applied to either adjacency or weighted graphs, the method is flexible enough to incorporate the data an analyst provides. A modification to the methods with the added place holder for a member and unknown location allows additional information to be considered and calculated.

3.5 Additive Preference Function

The Social, Operational and Location Criticality must now be combined to give a single Network Criticality measure for each group member. Thus, weights must be determined either with SME swing weight inputs, SME ranking or another method discussed in Section 2.5.2. In the event other weighting methods are not desired, the

three components can be weighted equally. Once the weights are established, similar to Equation (3.5), the product of the weight with the corresponding criticality for member *i* are combined, as seen in Equation (3.12).

$$C_i = w_{social}\left(C_{i,social}\right) + w_{operational}\left(C_{i,operational}\right) + w_{location}\left(C_{i,location}\right) \qquad (3.12)$$

This provides a weighted measure, combining social, operational and temporal local factors to the importance of an operator to a particular operation. These measures can be used to help guide the allocation of scare resources, provide screening for the analyst, and serve as inputs to other approaches.

3.6 Conclusion

The importance or criticality of a group member is based on the additive value of one's social, operational and location criticality. Weights are used throughout this methodology and SME inputs are preferred, however alternative methods may be used if a SME is unavailable.

The social importance of an individual hinges on the ordering of calculations. Weights for the types of affiliations are needed regardless of the method used to combine the layers. The swing weights or ranking are the most preferred methods, since the proportional weights provide an opportunity to apply too much importance to an affiliation simply because the information is easier to collect. Hamill's application of the centrality measures to a weighted graph make the most sense, as relationships across various types of affiliation types carry different levels of importance to an individual. While information centrality provides a look at possible links between members, eigenvector centrality has been show to be *stable* under the assumption of imperfect data.

Ultimately the choice of centrality measure will depend on the type of information wanted or needed by the analyst.

The operational importance of the member must consider their role in the completion of tasks, their skills or expertise and their connection to materials. The normalized reciprocal of the eigenvector centrality applied to the member/task incidence matrix provide a quantitative means to determine task criticality. The measure is then attributed to the members with the ability to complete the task. The use of risk applied to terrorist organization operations allows the exploitation of probabilities, events trees and risk importance measures to determine the critical nature of the group's resources. Partitioning the outcome space into events which indicate the success or failure of an attack allows the application of reliability measures. The averaged combination of normalized Fussell-Vesely and Risk Achievement Worth measures offers an importance of mission essential resources, which in turn are attributed to the individuals possessing the connections to those items.

The location of a member or members during a given time can provide information about the group's operations and event/attack planning. A SME's interpretation of the location information would provide the best means to measure the location importance. When a SME is unavailable to provide such information, the normalized sum of multidimensional eigenvector centrality applied to a relation and location incidence matrix quantifies location importance. The flexibility of the method allows for weighted or unweighted relations among members.

The social, operational and location criticality are combined for each member by an additive function. This value can then be used to identify opportunities to effectively

disrupt the network. The removal or influence of an individual with a high criticality value, will potentially impact the group's social structure and operational effectiveness and thus provide a means to accomplish the goals established for combating terrorism.

4 Results and Analysis

4.1 Introduction

This chapter demonstrations the methodology presented in Chapter 3 via a case based study based on open source information concerning the US embassy bombings in East Africa occurring on August 7, 1998. The attacks were carried out by two cooperating al-Qaeda cells against the US embassies in Nairobi, Kenya and Dar es Salaam, Tanzania (Champagne, 2005). This analysis determines the member importance via the social connections, task contributions, materials and skills accessed and the presence at locations of importance. The meta-matrices displaying all member, skill, materials and task connections are provided in Appendix B.

The results of this analysis identify the individuals within the group, who, if influenced or removed, would have hampered the operational success of this event. These results are then compared to those suggested by Carley: degree and betweenness centralities, cognitive load and task exclusivity (2003: 5). Calculations of these four measures are via the Operational Risk Analysis software created by Carley and the Center for Computational Analysis of Social and Organizational Systems (CASOS) (2006).

4.2 Event Background

The background information provided in this section was adapted from a student working paper, based on a course taught by William Keller (Champagne, 2005). al-Qaeda operations in Africa are believed to have increased substantially with support to

extremists, in Somalia, to disrupt US and United Nations support to Somalian refugees (2005; 53). As early as 1993, possible attack targets were serveilled (2005; 54). Members who planned and conducted the attacks included:

- *Planners and Facilitators from al-Qaeda Leadership*: Osama Bin Laden, Mamdouh Salim, Ali Mohamed, Kherchtou, Khalid al-Fawwaz (Financier), Abouhlaima, Wahid el-Hage, Abdullah Ahmed Abdullah, Muhsin Musa Matwalli Atwah (Electrical Engineer)

- *Nairobi, Kenya Cell*: Mohamed Sadeek Odeh, Mohamed Rashed Daoud al-Owhali (Suicide Bomber), Fazul Abdullah Mohammed, Azzam (Suicide Bomber)

- *Dar es Salaam, Tanzania Cell*: Fahad Mohammed Ally Msalam, Mustafa Mohammed Fadhil, Khalfan Khamis Mohamed, Ahmed Khalfan Ghailani, Hamden Khalif Allah Awad (Suicide Bomber)

In 1994, el-Hage assumed control of the East Africa cell, but was replaced by Abdullah in 1997 when the US Federal Bureau of Investigation became suspicious of his activities (2005; 55). In June and July 1998, the two cells procured a house and vehicle for use in each attack (2005; 57-58). In late July 1998, members from both cells began grinding the explosive (TNT), which was mixed with aluminum powder and used in combination with oxygen tanks to increase the explosive effect (2005; 69). Atwah, who was an electrical engineer, assembled the bombs and wired the trucks to be used as vehicle borne improvised explosive devices (VBIED) (2005; 16). Most members of the cells were ordered to vacate the target areas prior to the attack date (2005; 57). Suicide bombers Azzam, al-Owhali and Awad proceeded to the targets on August 7, 1998. Both trucks encountered obstacles at the target sites, but detonated near the target sites (2005; 59-62). The attacks killed a total of 224 people, 213 in Nairobi, Kenya and 11 in Der es Salaam, Tanzania, not including the suicide bombers (2005; 68).

4.3 Social Importance

The analysis in this section aims to identify the critical members of the social network for the East African Embassy bombing cell. For this type of analysis, an in depth study is needed to uncover the nature of the relationships between members. The first obstacle encountered related to conflicting information found in various open source resources. Therefore the information used in this analysis is a compilation of data from multiple sources. The second difficulty came from the lack of information related to the nature of connections between members. While the members of this group are likely connected to the larger al-Qaeda network through the six affiliations described by Sageman, there is limited evidence that the sub-network of cell members are connected via these same affiliations; therefore only a subset of the original six layers will be modeled with additional layers to represent member connections in this illustration.

The subject matter experts (SME) consulted for this case study have years of experience in the intelligence field. Based on the recommendation of the SME, the affiliations used to connect the East Africa bombing cell included: Reverent Power, Training, Friend and Group Member. *Reverent Power* is designated for relationships which are based on a supervisor/subordinate or some legitimate power or influence based on the member's position in larger organization and within the cell. *Training* is a connection representing a trainer/trainee relationship to include religious, jihad, weapons and so forth. The *Friend* connection indicates a relationship beyond the attack coordination, referring to house mates, business partners, previous co-workers and other encounters before this event. Finally the *Group Member* links those who worked together for this attack, both within their sub-cell and across cells. Figure 12 represents

the social connections among group members; affiliation types are denoted in Appendix B.

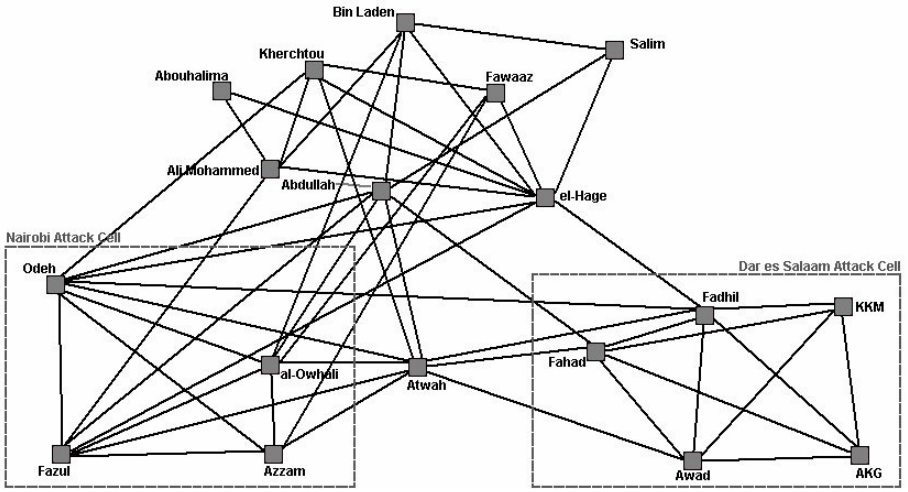


Figure 12 - Graphic of East Africa Embassy Attack Network

The SMEs found identifying the relative importance between affiliations difficult, however they were able to supply ranks for the affiliations within the sub-group; rank based weights for social networks, using Sageman's open source affiliations, are presented in Appendix C. The SMEs indicated there would be little difference between the *Reverent Power* and *Training* connections, therefore both carry equal weight. The sub-group affiliations, rank and weights are depicted in Table 17.

Table 17 - Sub-Group Affiliation Ranks & Weights

Affiliation	Rank	Weight
Reverent Power	1	0.36
Training	1	0.36
Friend	3	0.16
Group Member	4	0.12

The weights were calculated via the Rank Reciprocal rule as shown in Equation (3.3) with one variation. The items ranked third and fourth were calculated with the standard first to fourth ranking. The sum of the weights for items ranked third and fourth was

subtracted from one and the remainder was split equally between Reverent Power and Training, since they were considered equally important.

The resulting weighted connections matrix, based on the combination of layers as described by Hamill, is presented in Appendix B. The normalized and non-normalized eigenvector centrality scores for each member, developed from the weighted connections are shown in Table 18.

Table 18 - Member Criticality: Normalized Eigenvector Centrality

Member	Eigenvector Centrality	Normalized Eigenvector Centrality
Mohamed Sadeek Odeh	0.430	0.114
Fazul Abdullah Mohammed	0.391	0.104
Wadih el-Hage	0.334	0.089
Abdullah Ahmed Abdullah	0.326	0.086
Mohamed Rashed Daoud al-Owhali	0.309	0.082
Mustafa Mohammed Fadhil	0.237	0.063
Muhsin Musa Matwalli Atwah	0.221	0.059
Azzam	0.209	0.056
Osama Bin Laden	0.209	0.055
Ali Mohammed	0.183	0.048
Kherchtou	0.177	0.047
Fahad Mohammed Ally Msalam	0.167	0.044
Khalid al-Fawwaz	0.153	0.041
Mamdouh Salim	0.129	0.034
Khalfan Khamis Mohamed	0.103	0.027
Ahmed Khalfan Ghailani	0.080	0.021
Hamden Khalif Allah Awad	0.068	0.018
Abouhalima	0.044	0.012

Based on the number and nature of the weighted relationships, the results of Table 18 are consistent with what would be expected assuming undirected connections between members. Odeh and Fazul were clearly well connected to those in both attack cells and to those in the larger organization. El-Hage and Abdullah were also well connected; this is consistent with open source information, as el-Hage was the leader of al-Qaeda in Africa and was replaced by Abdullah, who is said to be the "mastermind" of the coordinated attack (Champagne, 2005: 57). Finally, Azzam and Awad, the suicide

bombers, were not well connected to the rest of the members, as they had limited roles in the preparations of the attacks. Others in leadership positions appear to have less influence or prestige; however this may be attributed to the OPSEC practices of the group.

4.4 Operational Importance

The operational criticality is comprised of two parts: the *task* criticality and *materials* and *skill* criticality. To calculate the task criticality, the member/task incidence matrix or assignment network from the meta-matrix is needed (as seen in Appendix B). The resource criticality requires a reliability/accessibility measure for each component of an operation.

4.4.1 Task Criticality

In approximately August 1997, the East Africa cell received funds and was ordered to begin preparations for an attack (Champagne, 2005: 57). The tasks identified in this attack included: surveillance, weapons training, driving, bomb preparation and bomb detonation. Again, the incidence matrix indicates the individuals capable of completing the task; it should be noted that while some members had weapons training, they were not considered for the bomb preparation due to their location.

Through the application of the multidimensional centrality, as presented in Section 3.3.1, the task criticality values were determined, as seen in Table 19.

Table 19 - Task Criticality: Normalized Eigenvector Centrality

Task	Eigenvector Centrality	Normalized Reciprocal of Eigenvector
surveillance	0.17	0.35
driving	0.22	0.28
bomb detonation	0.38	0.16
bomb preparation	0.49	0.12
weapons training	0.74	0.08

The results seemed contradictory to the initial argument that the fewer number of people capable of a task increases the task's criticality, since fewer members had driving training. However, after reviewing the individuals with surveillance training, two of the leaders/organizers conducted the surveillance and did not participate in other tasks. Hence, the removal of these two individuals would have likely interrupted, delayed, or lower the likelihood of the success of this operation.

4.4.2 Skills and Materials Criticality

The materials and skills are combined in an event tree to determine the individual contributions to the likelihood of the attack's success. The reliability of the explosive (bomb) and the bomber are conditional on the weapons expertise and availability of the target respectively. All other reliabilities are represented without the condition of other factors.

In the event analyzed here, the funds, facility and truck were materials which either were available and adequate for use or not. The money was used for the procurement of a facility, vehicle and explosives materials; the likelihood of being unavailable is very low due to various alternate sources of funds. The main facility concern was the ability to work undetected. There was a problem with the facility in Tanzania; however the effects to the attack were minimal (Champagne, 2005: 58); the time line for the attack

may have been impacted, but the remainder of the plan was unaffected. The truck needed only to operate and conceal the explosive.

The remainder of the components included: weapons expertise, bomb, target surveillance and bomber. Based on the explosive materials used (ground TNT), the likelihood of the bomb detonating properly was dependent on the expertise of the bomb maker. This difference is reflected in the event tree. Likewise, the bomber was more likely to detonate the bomb given that the target was accessible; this was evident in the Nairobi attack, as al-Owhali, one of the suicide bombers, exited the truck and ultimately was not killed in the attack (Champagne, 2005: 61). Though in both cases the target was inaccessible due to obstacles, the attacks were successful in taking lives and spreading fear.

The event tree, including all components, likelihoods and outcomes is displayed in Figure 13. The basic event probabilities for this case study are notational, though are based loosely on intelligence analysis of similar previous events and al-Qaeda operations.

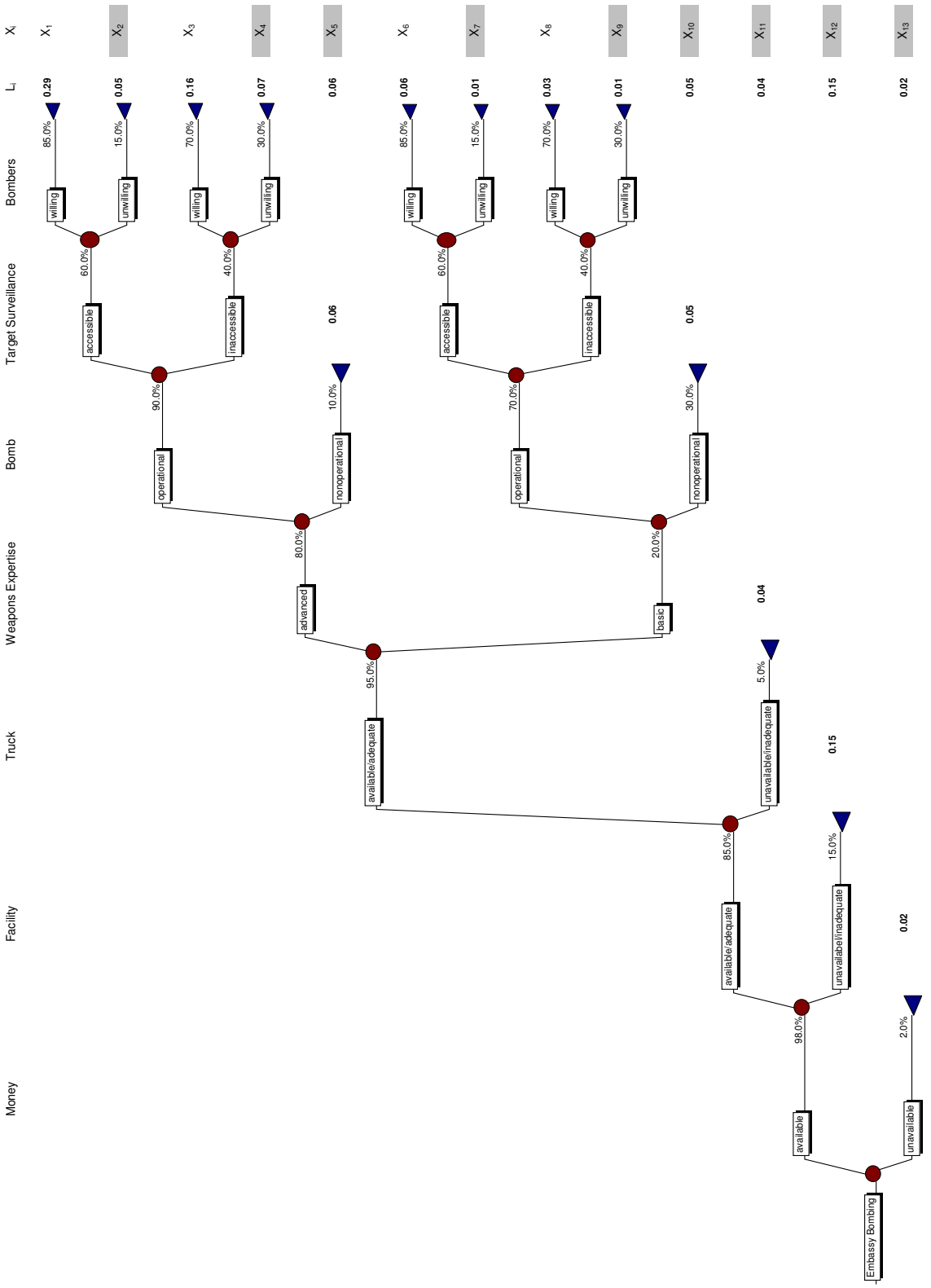


Figure 13 - Event Tree for East Africa Embassy Bombings

The outcomes (X_i) shaded gray denote a failure. The outcome space is reduced to the following, where *S* represents a success and *F* represents a failure:

$$S = \{X_1, X_3, X_6, X_8\}$$
$$F = \{X_2, X_4, X_5, X_7, X_9, X_{10}, X_{11}, X_{12}, X_{13}\}$$

The estimated likelihood of a successful attack was 54% and likelihood of failure was 46%.

The risk importance of each of the material and skill components needed for the attack are calculated via the Fussell-Vesely and Risk Achievement Worth measures as described in Section 3.3.3. The criticality is taken as the average of the two measures, as seen in Table 20 .

Table 20 - Material and Skill Criticality:

Resource	Fussell-Vesely	RAW	Normalized Fussell - Vesely	Normalized RAW	Average
Bomber Willingness	0.30	2.17	0.33	0.16	0.25
Facility	0.20	2.17	0.21	0.16	0.19
Bomb	0.20	2.17	0.21	0.16	0.19
Truck	0.07	2.17	0.07	0.16	0.12
Money	0.02	2.17	0.02	0.16	0.09
Surveillance	0.09	1.13	0.10	0.09	0.09
Weapons Expertise	0.04	1.22	0.05	0.09	0.07

Finally, the task, material and skill importance scores are combined with the information in the member/task, member/material and member/skill incidence matrices as seen in Equation (3.11). The resulting operational criticality score for each member is depicted in Table 21.

Table 21 - Operational Criticality

Member	Normalized Reciprocal Task Eigenvector Centrality	Risk Importance Measure Scores	Normalized Operational Criticality
Fazul Abdullah Mohammed	0.650	0.788	0.132
Azzam	0.875	0.409	0.118
Mohamed Rashed Daoud al-Owhali	0.594	0.409	0.092
Khalfan Khamis Mohamed	0.369	0.599	0.089
Abdullah Ahmed Abdullah	0.350	0.587	0.086
Mohamed Sadeek Odeh	0.207	0.599	0.074
Ali Mohammed	0.350	0.339	0.063
Hamden Khalif Allah Awad	0.442	0.249	0.063
Wadih el-Hage	0.083	0.508	0.054
Mamdouh Salim	0.083	0.413	0.045
Ahmed Khalfan Ghailani	0.125	0.307	0.040
Mustafa Mohammed Fadhil	0.083	0.319	0.037
Fahad Mohammed Ally Msalam	0.207	0.189	0.036
Muhsin Musa Matwalli Atwah	0.207	0.189	0.036
Kherchtou	0.207	0.000	0.019
Osama Bin Laden	0.000	0.094	0.009
Khalid al-Fawwaz	0.000	0.094	0.009
Abouhalima	0.000	0.000	0.000

The results in Table 21, when compared with those in Table 18, show the criticality of Fazul and Khalfan Mohamed, for this operation, increased due to their role in preparation of the attack. In addition, near the top are two of the three suicide bombers, signifying their criticality to the operations. The surprising result was the score for Atwah; he was solely responsible for assembling the explosives to the detonating devices, as he was the only reported electric engineer among the group. This suggests an additional task and skill should be added to account for the importance of connecting the bomb for detonation and the electrical skills. This change provides the new weights for the task, materials and skills, as displayed in Table 22.

Table 22 - Updated Task and Materials/Skills Scores

Task Criticality		Materials/Skills Criticality	
Task	Importance	Materials/Skills	Importance
Bomb Assembly	0.46	Electrical Engineer	0.22
Surveillance	0.19	Bomber	0.19
Drive	0.15	Facility	0.14
Bomb Detonation	0.09	Bomb	0.14
Bomb Preparation	0.07	Truck	0.09
Weapons Training	0.04	Money	0.08
		Weapons Expertise	0.07
		Surveillance	0.07

Based on the results of the weights in Table 22, Table 23 represents the updated member criticality based on their operational contributions. With the addition of bomb assembly as a task and electrical engineering as a skill, Atwah is one of the most important members of this operation. This change demonstrates the importance of identifying all critical tasks, materials and skills in an operation, as well as the flexibility to investigate and possibly update results that conflict with SME opinion and other intelligence analysis.

Table 23 - Updated Operational Criticality

Member	Normalized Reciprocal Task Eigenvector Centrality	Risk Importance Measure Scores	**Normalized Operational Criticality**
Fazul Abdullah Mohammed	0.350	0.610	0.119
Muhsin Musa Matwalli Atwah	0.570	0.360	0.116
Azzam	0.470	0.330	0.100
Khalfan Khamis Mohamed	0.200	0.470	0.083
Mohamed Rashed Daoud al-Owhali	0.320	0.330	0.081
Abdullah Ahmed Abdullah	0.190	0.440	0.078
Mohamed Sadeek Odeh	0.110	0.470	0.072
Ali Mohammed	0.190	0.260	0.056
Wadih el-Hage	0.040	0.400	0.055
Hamden Khalif Allah Awad	0.240	0.190	0.053
Mamdouh Salim	0.040	0.340	0.047
Ahmed Khalfan Ghailani	0.070	0.230	0.037
Mustafa Mohammed Fadhil	0.040	0.260	0.037
Fahad Mohammed Ally Msalam	0.110	0.140	0.031
Kherchtou	0.110	0.000	0.014
Osama Bin Laden	0.000	0.080	0.010
Khalid al-Fawwaz	0.000	0.080	0.010
Abouhalima	0.000	0.000	0.000

Further, the removal of the bomb maker would also affect other future operations. Finally, this update suggests the importance of identifying the key factors and a review by knowledgeable experts; factors may be removed later if found to be insignificant, but the omission of potentially critical factors could provide misleading results.

4.5 Time and Location

Finally, the locations of these members were noted at various times and places. The location of the group's members provides insight into the nature of their connections, locations of meetings, bases for operations and potential targets. For the purpose of this analysis, the following were used to identify the location criticality of members:

- Khartoum, Sudan – 1993
- Somalia – 1993
- Kenya – 1997
- Pakistan - June 1998
- Kenya – Spring –Summer 1998
- Kenya – Late July/Early August 1998
- Tanzania – Late July/Early August 1998
- Karachi, Pakistan – August 7, 1998
- Kenya – August 7, 1998
- Tanzania – August 7, 1998

The table containing the location of members is included in Appendix B.

The member/connection weighted matrix was created to reflect the meetings between members at the locations and times listed above using the method described in

Section 3.4. Applying the multidimensional centrality, as in Section 2.3.2, the importance of each location is noted in Table 24.

Table 24 - Location Importance

Location/Time	Normalized Eigenvector Centrality
Sudan - 1993	0.004
Somalia - 1993	0.072
Kenya - 1997	0.104
Pakistan - June 1998	0.010
Kenya - Spring/Summer 1998	0.030
Tanzania - Spring/Summer 1998	0.085
Kenya - July/Aug 1998	0.199
Tanzania - July/Aug 1998	0.339
Pakistan - Aug 7, 1998	0.092
Kenya - Aug 7, 1998	0.025
Tanzaniz - Aug 7, 1998	0.001
Location Unknown	0.037

The importance values gained from these results indicates that Tanzania and Kenya in late July and early August were most important; the higher value for Tanzania supports the information that this attack was planned on a shorter timeline than the Kenya attack, as attack preparations were conducted closer to the attack date (Champagne, 2005; 55). The importance attributed to each member based on their location at specific times and the normalized location criticalities are displayed in Table 25.

Table 25 - Normalized and Non-Normalized Location Criticality

Member	Location Criticality	Normalized Location Criticality
Muhsin Musa Matwalli Atwah	0.722	0.132
Fahad Mohammed Ally Msalam	0.620	0.114
Mustafa Mohammed Fadhil	0.516	0.095
Ahmed Khalfan Ghailani	0.516	0.095
Abdullah Ahmed Abdullah	0.505	0.093
Fazul Abdullah Mohammed	0.431	0.079
Khalfan Khamis Mohamed	0.425	0.078
Mohamed Sadeek Odeh	0.394	0.072
Hamden Khalif Allah Awad	0.377	0.069
Azzam	0.370	0.068
Mohamed Rashed Daoud al-Owhali	0.339	0.062
Wadih el-Hage	0.145	0.027
Khalid al-Fawwaz	0.072	0.013
Osama Bin Laden	0.010	0.002
Mamdouh Salim	0.004	0.001
Ali Mohammed	0.004	0.001
Kherchtou	0.000	0.000
Abouhalima	0.000	0.000

4.6 Additive Preference Function

To determine the overall criticality of each member, an additive preference function is used as described in Equation (2.16). The preference function combines the normalized values from Table 18, Table 23, and Table 25 and the weights provided by the SME. Due to the background of the SMEs and the time available, the "100 Ball" method was used to elicit the following weights: Social (.5), Operational (.3) and Location (.2). Using Equation (3.12), the final resulting criticality for each member is summarized in Table 26.

Table 26 - Total Member Criticality

Member	Normalized Social Eigenvector Centrality	Normalized Operational Criticality	Normalized Location Criticality	**Total Criticality**
Fazul Abdullah Mohammed	0.104	0.119	0.078	**0.103**
Mohamed Sadeek Odeh	0.114	0.072	0.072	**0.093**
Muhsin Musa Matwalli Atwah	0.059	0.116	0.132	**0.090**
Abdullah Ahmed Abdullah	0.086	0.078	0.093	**0.085**
Mohamed Rashed Daoud al-Owhali	0.082	0.081	0.062	**0.078**
Azzam	0.056	0.100	0.068	**0.071**
Wadih el-Hage	0.089	0.055	0.027	**0.066**
Mustafa Mohammed Fadhil	0.063	0.037	0.095	**0.062**
Khalfan Khamis Mohamed	0.032	0.083	0.078	**0.057**
Fahad Mohammed Ally Msalam	0.044	0.031	0.114	**0.054**
Ali Mohammed	0.048	0.056	0.001	**0.041**
Ahmed Khalfan Ghailani	0.021	0.037	0.095	**0.041**
Hamden Khalif Allah Awad	0.018	0.053	0.069	**0.039**
Mamdouh Salim	0.034	0.047	0.001	**0.031**
Osama Bin Laden	0.055	0.010	0.002	**0.031**
Kherchtou	0.047	0.014	0.000	**0.028**
Khalid al-Fawwaz	0.041	0.010	0.013	**0.026**
Abouhalima	0.012	0.000	0.000	**0.006**

The results in Table 26 show two of the Kenya cell members (Fazul and Odeh) as the most critical in this notional example. Since both of these individuals were included in attack preparations very early, their contributions were significant. Abdullah's role as the leader of the operation warrants the importance level. Atwah was a significant contributor to the operation, as shown by the criticality score.

4.7 Calculations in ORA

Using the meta-matrices, found in Appendix B, the four measures explained in Table 6 were calculated using the Organization Risk Analysis (ORA) software. One important difference between the calculations in this research and ORA is the weighted relationships; ORA accounts only for a relationship or the absence of a relationship and not the strength of the tie between members. The results for the Degree centrality, Betweenness centrality, Cognitive Load and Task Exclusivity are included in Table 27.

Table 27 - ORA Measure Results

Member	Deree Centrality	Betweenness Centrality	Cognitive Load/ Demand	Task Exclusivity
Osama Bin Laden	0.294	0.026	0.079	0.000
Mamdouh Salim	0.176	0.003	0.204	0.000
Ali Mohammed	0.294	0.028	0.128	0.008
Abouhalima	0.118	0.000	0.012	0.000
Kherchtou	0.294	0.019	0.178	0.001
Khalid al-Fawwaz	0.176	0.011	0.068	0.000
Abdullah Ahmed Abdullah	0.412	0.089	0.240	0.008
Wadih el-Hage	**0.529**	**0.253**	0.189	0.000
Mohamed Sadeek Odeh	*0.471*	0.061	0.295	0.001
Mohamed Rashed Daoud al-Owhali	0.412	0.043	0.259	0.011
Fazul Abdullah Mohammed	0.412	0.048	**0.371**	0.026
Azzam	0.294	0.010	0.295	*0.034*
Muhsin Musa Matwalli Atwah	*0.471*	0.128	0.256	**0.167**
Fahad Mohammed Ally Msalam	0.353	0.076	0.184	0.001
Mustafa Mohammed Fadhil	0.412	*0.198*	0.177	0.000
Khalfan Khamis Mohamed	0.235	0.000	*0.305*	0.003
Ahmed Khalfan Ghailani	0.235	0.000	0.186	0.001
Hamden Khalif Allah Awad	0.294	0.008	0.185	0.026

The two highest score for each measure, in Table 27, are shaded. The highest value is indicated in bold and the second highest is italicized. These results indicate that el-Hage had the highest number of social interactions, with no consideration for the strength of the relationships. El-Hage was removed from his leadership role early during preparations, due to attention from the US; his replacement by Abdullah ensured continued preparations were successful. Fazul scored the highest for cognitive demand, followed by Khalid. Due to the various knowledge and materials and the capability to complete many of the tasks, Fazul and Khalid were significant contributors. Finally, Atwah was critical due to his electrical engineering skills and Azzam' contributions, in the form of surveillance and the suicide bombing, were also important.

Portions of the results in this section are inconsistent with the findings of the methodology used in this research, though can likely be attributed to differences in the weighting of relations and the choice of centrality measures. el-Hage scored the highest

for the unweighted adjacencies used in the calculation of the Degree and Betweenness centralities in ORA, as seen in Table 27. The results of the Eigenvector centrality of the weighted relations placed el-Hage third, as seen in Table 18 and seventh for total criticality, seen in Table 26. Ultimately the identification of el-Hage as important, via centrality alone, reinforces the premise of this research; the removal of leaders and those with social prestige is not enough to destabilize terrorist networks or their operations. There is agreement between the two methods that Fazul was an important contributor, while Atwah was critical to the completion of the IEDs.

4.8 Conclusion

The al-Qaeda sub-cell operating in East Africa, conducted attacks on two US embassies in 1998. The social connections between group members provided the means to share skills and materials needed to successfully complete the tasks to conduct the attacks. This analysis identifies members critical to the network due to their social connections, operational contributions and proximity to meeting and attack locations. The result of this open source illustration shows that two of the top three members, with high criticality scores, were not leaders; Fazul and Atwah completed critical tasks aided by their skills and access to materials. The idea of destabilizing a network by the removal of members other than leaders is supported by Carley's incorporation of cognitive load/demand and task exclusivity (2003: 5). The identification of members, based on operational contributions, was consistent between the methodology use in this research and the ORA software.

This research is unique due to the efforts to combine Operations Research and Social Network theory with the perspectives of SMEs on current terrorist threats and events. The method used here to combine previously unrelated measures, provides a collective look at the group members' position, both socially and operationally, within the network. Ultimately, this research draws on multiple facets of a terrorist organization simultaneously, rather than separately.

The potential benefits from the use of this methodology are not limited to the identification of members for influence or removal in order to destabilize the terrorist organization. Members near the top are well connected socially and are important operational contributors, implying a level of trust within the organization. This could potentially indicate future leaders within the organization or for specific attacks. In addition, tracking changes in scores may signal potential operational activity even when their exact nature is not yet known. Locations where group members are known to frequent could provide the opportunity to gain insight into operations and future plans. Further, the location of cells, such as the East Africa cell, could indicate the need for increased security at potential target sites. Finally, the identification of the critical materials and skills would focus US and allied efforts to reduce the availability or reliability of such resources.

5 Conclusions

5.1 Overview of the Model

This thesis provides an approach to determine the criticality of clandestine group members to particular operations. This criticality is comprised of measures which account for a member's social importance, operational contributions and proximity to locations important to the organization. Social Network Analysis (SNA), specifically Eigenvector centrality, provides a proxy for the prestige or influence a member has within the group based on the members' relationships. This research draws on the contributions of Clark (2005) and Hamill (2006) to determine the strength of the relations between members base on the type of affiliations comprising the connection. Risk Analysis, specifically event trees and risk importance measures, were incorporated to analyze how the reliability and availability of resources contribute to the likelihood an attack will be successful. Multidimensional centrality provided the foundation for task criticality and location importance to be assigned to group members. Finally, an additive preference model combined the social, operational and location importance with a relative weight of each factor to give a total criticality score for each group member.

5.2 Objectives of this Study

The primary objective of this research was to provide analysts a method to identify clandestine group members who if influenced or removed from the network would impact the organization's operations. Limited open source research has been done to provide a comprehensive method for identifying the critical members of clandestine networks, hence this research combines multiple disciplines. Research applying SNA

theory to clandestine networks has been primarily due to the efforts of Carley and her colleagues. The Department of Defense and Homeland Security have employed risk analysis to identify and mitigate terrorist attack vulnerabilities within the United States, but few open source reports have focused on the vulnerabilities in clandestine operations. While the method presented in this research crudely combines the multiple facets of clandestine operations, it provides a starting point for future research.

5.3 Recommendations for Future Research

Since this research uniquely combines the social, operational and location importance of clandestine group members, there are a number of avenues available to improve calculations and better identify critical members. Improvements to the calculation of relationship strengths are imperative, as the social structure of the group provides the basis for operational success. Additional analysis of the risk associated with the organizations' operations would provide invaluable information. Finally, the incorporation of this method with others to prioritize members for influence or removal should be investigated.

First, this research assumed only positive factors as contributors to the strength of the relationship between group members. Further work with subject matter experts is needed to determine the *relative importance* between affiliations which contribute to the strength of relationships. Realistically, consideration should be given to factors which inhibit or degrade the relationships. These inhibiting factors may include differences between tribes, religious views, ethical or moral values, and or a member's commitment (Downs, 2006) to the group and the mission of the organization. Similarly, the model could then account for relations between members which inhibit effective operations.

Next, more work is needed to improve the risk analysis portion of this method. To begin, data is needed to calculate the reliability and availability of skills and materials associated with the group of interest. Additionally, categorical impacts, in terms of potential lives lost, could be tied to the outcomes of the event tree. This would provide the opportunity to calculate the Expected Value of Perfect Information (EVPI) to aid efforts to further destabilize operations via the resources. Sensitivity and uncertainty analysis would provide insight into how varied basic event probabilities would change a member's criticality.

Finally, the criticality of members should be combined with other methods to prioritize members for targeting. Creating a multi-criteria problem with the criticality, developed in this research, and a member's commitment, as developed by Downs (2006), would distinguish members who should considered for influence and those who should be removed from the network. Balancing the strength of a relationship with the likelihood the relationship truly exists, as formulated by Seder (2007), could aid in decreasing the effects of imperfect data. The weighted relations in this research could be combined with Herbranson's (2007) efforts to create network disruption target sets. Ultimately, this method could provide the node criticality and arc weights to optimally cut the network into disjoint subsets, destabilizing all social and operational ties.

5.4 Conclusion

The need to destabilize clandestine networks, especially terrorist groups, is not likely to decrease in the coming years. Research must continue to develop methods for identifying and targeting the members of these organizations in order to decrease their operational success. Efforts to remove the leaders of terrorist groups have proved

ineffective, as other capable members willingly replace them. The key to stifling the operational reach of these terrorist groups lies in the resources. While many analyses currently focus on only the social connections and structures of these groups, it is the incorporation of the operational and location information that strengthens this approach.

Appendix A - CBRN Components

The information contained in this appendix, focuses specifically on the components needed for chemical, biological, radiological and nuclear (CBRN) weapons. These components will provide insight into the possible tasks, materials and knowledge associated with the use of CBRN weapons in operations. The information in this section is extracted from *A Military Guide to Terrorism in the Twenty-First Century* (USTRADOC, 2005). The guide suggests that as we create counters for the current tactics used by terrorists, they will begin to convert to more extreme tactics and weapons.

A.1 Chemical Weapons

Chemical weapons, as defined by the Department of Defense (DoD Dictionary, 2001) are:

> "Together or separately, (a) a toxic chemical and its precursors, except when intended for a purpose not prohibited under the Chemical Weapons Convention; (b) a munition or device, specifically designed to cause death or other harm through toxic properties of those chemicals specified in (a), above, which would be released as a result of the employment of such munition or device; (c) any equipment specifically designed for use directly in connection with the employment of munitions or devices specified in (b), above."

Chemical agents are categorized based on their effect (lethality) and persistence (length of effect). Examples of chemical agents are included in Table 28.

Table 28 - Chemical Agents (US Army TRADOC, 2005:G-4,G-5)

Agent	Lethal	Symbol Name
Nerve	Yes	G Series, GB/Sarin, GD/Soman (VR 55)
	Yes	V Agent
Blood	Yes	AC/Hydrogen Cyanide
Blister	Yes	HD/Mustard, HN/ Nitrogen Mustard, L/Lewisite, HL/Mustard & Lewisite, CX/Phosgene Oxime
Choking	Yes	CG/Phosgene, DP/Diphosagene
Incapacitant	No	BZ
Irritant	No	DA/Diphenyl Chloroarsine, DM/Adamsite, CN/Chloro-acetophenone, CS/O-Chloro-benzylidene-malononitrile, PS/Chloropicrin

To determine the risk associated with chemical weapons, consideration must be given to the dissemination methods, quantity available/accessible either by purchase or theft, and the possible use of an explosive weapon in conjunction with the chemicals. Dissemination adds a level of complexity to the release of such an agent, since the dispersion can be impacted by wind and temperature changes. A release into the environment affects the integrity of the agent and requires a larger quantity of the agent to create the desired effect. Possible delivery methods include: mortars, bombs carried in vehicles or backpacks, and long term burst capabilities in the form of vapor or aerosol from sprayers or canisters. Finally, toxic industrial chemicals used in large quantities could produce similar results and are more readily available.

A.2 Biological Weapons

The DoD definition of biological weapons is “An item of materiel which projects, disperses, or disseminates a biological agent including arthropod vectors” (DoD Dictionary, 2001). Biological weapons include: pathogenic microbes, toxins and bioregulators (Table 29).

Table 29 - Biological Agents (US Army TRADOC, 2005: G-9)

Pathogens	Toxins	Bioregulators
Anthrax	Mycotoxins	Neurotransmitters
Cholera	Venoms	Hormones
Plague	Shell Fish	Enzymes
Smallpox	Botulinum	
Tularemia	Ricin	
Influenza		
Fevers		

Smaller amounts of biological agents are required to achieve the same effect as much larger quantities of chemical agents. Biological agents cost less and are more readily available. Toxins require an individual familiar with genetic engineering in order to produce or reproduce. Dissemination of biological agents is best achieved in liquid or powder forms. Other dissemination methods include: sprayers or aerosol transported via cars, trucks or ships; through heating, ventilation or air conditioning; and water or food sources.

A.3 Radiological Weapons

The DoD definition of radiological operation is defined as:

> "The employment of radioactive materials or radiation producing devices to cause casualties or restrict the use of terrain. It includes the intentional employment of fallout from nuclear weapons (DoD Dictionary, 2001).

The use of radiological contaminants requires access to materials in either a stable or unstable state. The use of radiological materials in industry, agriculture, and public arenas increases the potential for access. A common dispersion method uses a radiological dispersal device (RDD). The DoD defines a radiological dispersal device as: "A device, other than a nuclear explosive device, designed to disseminate radioactive material in order to cause destruction, damage, or injury" (DoD Dictionary, 2001). Radiological materials combined with conventional explosive weapons would result in a

dirty bomb, as a means of dispersion. Models currently considering the risk associated with radiological weapons account for: quantity of the material, specific radiological material and the size of its particles, the dispersal technique, wind speed and weather conditions, and urban building composition and population densities. Attacks on the physical location of reactors are yet another option of the dispersion of radiological materials.

A.4 Nuclear Weapons

The DoD defines nuclear weapon as:

> "A complete assembly (i.e., implosion type, gun type, or thermonuclear type), in its intended ultimate configuration which, upon completion of the prescribed arming, fusing, and firing sequence, is capable of producing the intended nuclear reaction and release of energy" (DoD Dictionary, 2001).

Limitations on money and technical resources create the greatest potential for the use of nuclear weapons to fail. The technical skills needed for a weapon of this type includes individuals familiar with nuclear physics, among other skills. In order to use a material, such as plutonium, it must be stolen or purchased. The type of nuclear material dictates the quantity need for an effective attack. Specialized skills are required to assemble a device if it is produced. Specific materials and parts are required. However, if a complete weapon were acquired, some of these requirements would not be necessary. Transportation generally needs the means to conceal the bulky bomb and material. Transportation methods include: trucks, vehicles or ships used for shipping.

Appendix B - Illustration Data Tables

The information contained in this appendix is used throughout Chapter 4 for the notional example. The information pertaining to members, skills, materials, tasks are arranged according to the meta-matrix described in Section 2.3.3. This appendix also includes the following: weighted communications network matrix (used in Section 4.3) and the time and location information (used in Section 4.6). The data contained in this section is the fused product of a data set available on the Computational Analysis of Social and Organizational System (CASOS) website, event and member information available via wikipedia, and *Anatomy of a Terrorist Attack* (Champagne, 2005).

B.1 Communications Network (Member/Member)

This section contains a table representing the types of affiliations which comprise the relationships between members. Table 30 shows the connections between members based on the various types of affiliations (r = reverent power, t = training, f = friend, g = group member).

Table 30 - Communication Network

	OBL	Salim	Ali Mohammed	Abouhalima	Kherchtou	Fawwaz	AAA	el-Hage	Odeh	al-Owhali	Fazul	Azzam	Atwah	Fahad	Fadhil	KKM	AKGhailani	Awad
OBL		r,f	r				r,g	r,g		t								
Salim	r,f						r	r										
Ali Mohammed	r			t	t			f			r,t							
Abouhalima			t					f										
Kherchtou			t			r		r,g	t				t					
Fawwaz					r			r										
AAA	r,g	r							r,g	r,g	r,g		r,g	r,g				
el-Hage	r,g	r	f	f	r	r			r,f,g		r,g				r,g			
Odeh					t		r,g	r,f,g		r,g	r,f,g	r,g	g,t		r,g			
al-Owhali	t						r,g		r,g		r,f,g	f,g	g					
Fazul			r,t				r,g	r,g	r,f,g	r,f,g		r,g	g					
Azzam									r,g	f,g	r,g		g					
Atwah					t		r,g		g,t	g	g	g		g	g			g
Fahad							r,g						g		r,f,g	r,f,g	r,g	g
Fadhil								r,g	r,g				g	r,f,g		r,f,g	r,g	r,g
KKM														r,f,g	r,f,g		g	g
AKGhailani														r,g	r,g	g		g
Awad													g	g	r,g	g	g	

The strength of the relationships between members is based on weights for reverent power (.36), trainer (.36), friend (.16), and group member (.12). The weighted connections between members are represented in Table 31.

Table 31 - Weighted Communications Network

	OBL	Salim	Ali Mohammed	Abouhalima	Kherchtou	Fawwaz	AAA	el-Hage	Odeh	al-Owhali	Fazul	Azzam	Atwah	Fahad	Fadhil	KKM	AKGhailani	Awad
OBL	0	0.52	0.36	0	0	0	0.48	0.48	0	0.36	0	0	0	0	0	0	0	0
Salim	0.52	0	0	0	0	0	0.36	0.36	0	0	0	0	0	0	0	0	0	0
Ali Mohammed	0.36	0	0	0.36	0.36	0	0	0.16	0	0	0.72	0	0	0	0	0	0	0
Abouhalima	0	0	0.36	0	0	0	0	0.16	0	0	0	0	0	0	0	0	0	0
Kherchtou	0	0	0.36	0	0	0.36	0	0.36	0.36	0	0	0	0.36	0	0	0	0	0
Fawwaz	0	0	0	0	0.36	0	0	0.48	0	0.36	0	0.36	0	0	0	0	0	0
AAA	0.48	0.36	0	0	0	0	0	0	0.48	0.48	0.48	0	0.48	0.48	0	0	0	0
el-Hage	0.48	0.36	0.16	0.16	0.36	0.48	0	0	0.64	0	0.48	0	0	0	0.48	0	0	0
Odeh	0	0	0	0	0.36	0	0.48	0.64	0	0.48	0.64	0.48	0.48	0	0.48	0	0	0
al-Owhali	0.36	0	0	0	0	0.36	0.48	0	0.48	0	0.64	0.28	0.12	0	0	0	0	0
Fazul	0	0	0.72	0	0	0	0.48	0.48	0.64	0.64	0	0.48	0.12	0	0	0	0	0
Azzam	0	0	0	0	0	0.36	0	0	0.48	0.28	0.48	0	0.12	0	0	0	0	0
Atwah	0	0	0	0	0.36	0	0.48	0	0.48	0.12	0.12	0.12	0	0.12	0.12	0	0	0.12
Fahad	0	0	0	0	0	0	0.48	0	0	0	0	0	0.12	0	0.64	0.64	0.48	0.12
Fadhil	0	0	0	0	0	0	0	0.48	0.48	0	0	0	0.12	0.64	0	0.64	0.48	0.48
KKM	0	0	0	0	0	0	0	0	0	0	0	0	0	0.64	0.64	0	0.12	0.12
AKGhailani	0	0	0	0	0	0	0	0	0	0	0	0	0	0.48	0.48	0.12	0	0.12
Awad	0	0	0	0	0	0	0	0	0	0	0	0	0.12	0.12	0.48	0.12	0.12	0

B.2 Knowledge Network (Member/Knowledge)

The member/knowledge incidence matrix includes members representing the rows and columns representing a knowledge or skill. A one indicates the member had the knowledge or skill, while a zero indicates they did not. Table 32 shows the skills each member was reported to possess, represented by a one under the appropriate task column.

Table 32 - Knowledge Network

Member	Weapons Expertise	Surveillance	Bomber Mindset	Electrical Engineer
OBL	0	0	0	0
Salim	1	0	1	0
Ali Mohammed	0	1	1	0
Abouhalima	0	0	0	0
Kherchtou	0	0	0	0
Fawwaz	0	0	0	0
AAA	0	1	0	0
el-Hage	1	0	1	0
Odeh	1	1	1	0
al-Owhali	1	1	1	0
Fazul	1	1	1	0
Azzam	1	1	1	0
Atwah	0	0	0	1
Fahad	0	0	0	0
Fadhil	1	0	1	0
KKM	1	1	1	0
AKGhailani	0	0	0	0
Awad	0	0	1	0

B.3 Capabilities Network

The member/materials incidence matrix, in this section, indicates the materials accessible to each member. The resources or materials accessible to each member are displayed in Table 33 with a one in the indicated in the appropriate column.

Table 33 - Capabilities Network

Member	Money	Facility	Truck	Bomb/Explosives
OBL	1	0	0	0
Salim	1	0	0	0
Ali Mohammed	0	0	0	0
Abouhalima	0	0	0	0
Kherchtou	0	0	0	0
Fawwaz	1	0	0	0
AAA	0	1	1	1
el-Hage	0	0	0	1
Odeh	0	1	0	0
al-Owhali	0	0	0	0
Fazul	0	1	0	1
Azzam	0	0	0	0
Atwah	0	0	0	1
Fahad	0	1	0	0
Fadhil	0	0	0	0
KKM	0	1	0	0
AKGhailani	0	1	1	0
Awad	0	0	0	0

B.4 Assignment Network

The member/task incidence matrix accounts for the tasks a member is capable of completing and not necessarily those a member is assigned to complete. The assignment network represented in Table 34, includes a one for the tasks each member is capable of completing.

Table 34 - Assignment Network

Member	Surveillance	Weapons Training	Drive	Bomb Preparation	Bomb Connection	Bomb Detonation
OBL	0	0	0	0	0	0
Salim	0	1	0	0	0	0
Ali Mohammed	1	0	0	0	0	0
Abouhalima	0	0	0	0	0	0
Kherchtou	0	1	0	1	0	0
Fawwaz	0	0	0	0	0	0
AAA	1	0	0	0	0	0
el-Hage	0	1	0	0	0	0
Odeh	0	1	0	1	0	0
al-Owhali	1	1	0	0	0	1
Fazul	0	1	1	1	0	1
Azzam	1	1	1	0	0	1
Atwah	0	1	0	1	1	0
Fahad	0	1	0	1	0	0
Fadhil	0	1	0	0	0	0
KKM	0	1	0	1	0	1
AKGhailani	0	0	0	1	0	0
Awad	0	0	1	0	0	1

B.5 Knowledge Requirements Network

The knowledge/task incidence matrix represents the knowledge and skills as rows and the task as columns. The knowledge requirements network displayed in Table 35, indicates the skills or knowledge required for each task with a one.

Table 35 - Knowledge Requirements Network

Task / Knowledge	Surveillance	Weapons Training	Drive	Bomb Preparation	Bomb Connection	Bomb Detonation
Weapons Expertise	0	1	0	0	0	1
Surveillance	1	0	0	1	1	0
Bomber Mindset	0	0	0	0	0	0
Electrical Engineer	0	0	0	0	1	0

B.6 Resource Requirements Network

Similar to the knowledge requirements network, the resource requirements network represents materials as rows and tasks as columns. The resource requirements network accounts for the resources associate with each task, as seen in Table 36.

Table 36 - Resource Requirements Network

Task / Materials	Surveillance	Weapons Training	Drive	Bomb Preparation	Bomb Connection	Bomb Detonation
Money	0	0	0	0	0	1
Facility	0	0	0	1	1	0
Truck	0	0	1	0	0	1
Bomb/Explosives	0	1	0	1	1	0

B.7 Precedence Network

A one in this precedence matrix indicates that the task representing the column must be completed before the task represented in the row. The precedence network shows the order in which tasks much be completed, shown in Table 37.

Table 37 - Task Precedence Network

Tasks	Surveillance	Weapons Training	Drive	Bomb Preparation	Bomb Connection	Bomb Detonation
Surveillance	0	0	0	0	0	0
Weapons Training	0	0	0	0	0	0
Drive	0	0	0	0	0	0
Bomb Preparation	0	1	0	0	0	0
Bomb Connection	0	0	0	1	0	0
Bomb Detonation	0	0	0	0	1	0

B.8 Locations

Information contained in Table 38 includes the reported time and location of the members described in Section 4.5. The *unk* included in bold represent important time periods when the unknown location of members was potentially important. The non-bolded *unk* is used for members who contributed little to the preparations and operation and therefore were not included in the analysis (Section 4.5).

Table 38 - Location Matrix

	Spring 1993	Summer 1997	Spring-Summer 1998	Late July - Early Aug	Attack
Osama Bin Laden	unk	unk	Pakistan	unk	unk
Mamdouh Salim	Khartoum, Sudan	Khartoum, Sudan	Bosnia	unk	unk
Ali Mohammed	Khartoum, Sudan	unk	unk	unk	unk
Wadih el-Hage	Khartoum, Sudan	Kenya	**unk**	United States	United States
Abdullan Ahmed Abdullah	Somalia	Kenya	**unk**	Kenya	Karachi, Pakistan
Khalid al-Fawwaz	Kenya	United Kingdom	United Kingdom	unk	unk
Muhsin Musa Matwalli Atwah	Somalia	**unk**	**unk**	Kenya, Tanzania	**unk**
Mohamed Sadeek Odeh	Somalia	Somalia	Kenya	Kenya	Karachi, Pakistan
Mohamed Rashed Daoud al-Owhali	unk	Kenya	Pakistan	Kenya	Kenya
Fazul Abdullah Mohammed	Somalia	Kenya	Sudan, Kenya	Kenya	Kenya
Azzam	unk	Kenya	Pakistan, Kenya	Kenya	Kenya
Fahad Mohammed Ally Msalam	unk	Kenya	Tanzania	Tanzania	Karachi, Pakistan
Mustafa Mohammed Fadhil	unk	unk	Tanzania	Tanzania	Karachi, Pakistan
Khalfan Khamis Mohamed	unk	unk	Tanzania	Tanzania	Tanzania
Ahmed Khalfan Ghailani	unk	unk	Tanzania	Tanzania	Karachi, Pakistan
Hamden Khalif Allah Awad	unk	unk	**unk**	Tanzania	Tanzania
Kherchtou	unk	unk	unk	unk	unk
Abouhalima	unk	unk	unk	unk	unk

Appendix C - Affiliation Weights Across Cultures

The subject matter experts (SME), who provided the affiliation rank in the example in Section 4.3, were able to confirm the assertion in Section 3.2.1; the type of affiliation constituting a relationship, are valued approximately the same across cultures. The SMEs, who have many years of intelligence experience, were able to provide affiliations values for the Muslim, Sub-Sahara and South American cultures. Table 39 provides the ordinal ranking of the affiliations identified by Sageman for each culture.

Table 39 - Multi-Cultural Ordinal Ranks of Affiliations

	Muslim	Sub-Sahara	South America
Nuclear Family	1	1	1
Extended Family	2	2	2
Friends	3	3	3
Worship	4	5	4
Discipleship	5	4	5
Extended Friends/ Acquaitances	6	6	6

Using the rank reciprocal rule, Equation (2.17), the weight associate with the rank of each affiliation for each culture, found in Table 39, is displayed in Table 40.

Table 40 - Multi-Cultural Weight of Affiliations

	Muslim	Sub-Sahara	South America
Nuclear Family	0.41	0.41	0.31
Extended Family	0.20	0.20	0.31
Friends	0.14	0.14	0.14
Worship	0.10	0.08	0.10
Discipleship	0.08	0.10	0.08
Extended Friends/ Acquaitances	0.07	0.07	0.07

Figure 14 provides a graphic depiction of weights for each affiliations and culture, based on the rank reciprocal rule.

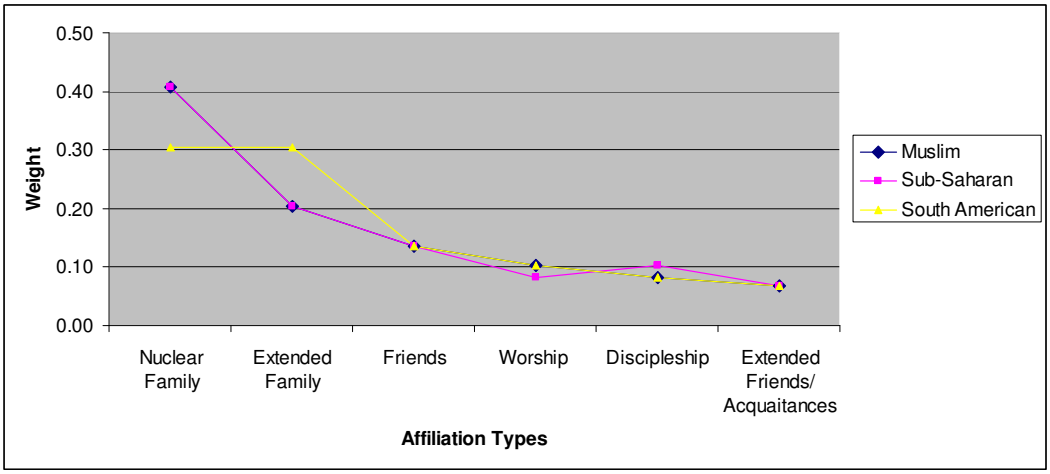


Figure 14 - Multi-Cultural Values of Affiliations

Bibliography

Baker, Wayne E. and Robert R. Faulkner. "The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry," *American Sociological Review,* 58 (6): 837 – 860 (December 1993).

Bedford, Tim and Roger Cooke. *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge UK: Cambridge University Press, 2001.

Bonacich, Philip. "Power and Centrality: A Family of Measures," *American Journal of Sociology,* 92(5): 1170-1182 (March 1987).

Bonacich, Philip, Annie C. Holdren and Michael Johnston. "Hyper-edges and Multidimensional Centrality," *Social Networks,* 26(3): 189-203 (July 2004).

Bonacich, Phillip and Paulette Lloyd. "Eigenvector-like Measures of Centrality for Asymmetric Relations," *Social Networks,* 23(3):191-201 (July 2001).

Borgatti, Stephen P. "Centrality and Network Flow," *Social Networks,* 27: 55-71 (2005).

Borgatti, Stephen P., Kathleen M. Carley and David Krackhardt. "On the Robustness of Centrality Measures Under Conditions of Imperfect Data," S*ocial Networks*, 28: 124-136 (2006).

Bottomley, Paul A., John R. Doyle and Rodney H. Green. "Testing the Reliability of Weight Elicitation Methods: Direct Rating Versus Point Allocation," *Journal of Marketing Research*, XXXXII: 508-513 (November 2000).

Buchanan, Mark. *Nexus: Small Worlds and the Groundbreaking Science of Networks*. New York: Norton, 2002.

Bush, George W., President, United States of America. "Freedom at War with Fear." Address to a Joint Session of Congress and the American People. United States Capitol, Washington, D.C. 20 September, 2001

Carley, Kathleen. "Summary of Key Measures for Characterizing Organizational Architectures," Working Paper. Center for Computational Analysis of Social and Organizational Systems (August 2001). Carnegie Mellon University, Pittsburg, PA. http://www.casos.cs.cmu.edu/publications/papers/MeasuresInfo.pdf (retrieved: 1 March 2007)

Carley, Kathleen and Matt DeReno. *ORA 2006: User's Guide*. CMU-ISRI-06-113. Pittsburg PA: CASOS, August 2006.

Carley, Kathleen , Douglas Fridsma, Elizabeth Casman, Alex Yahja, Neal Altman, Li-Choiu Chen, Boris Kaminsky, and Demian Nave. "BioWar: Scalable Agent-Based Model of Bioattacks," *IEEE Transactions on Systems, Man and Cybernetics – Part A: Systems and Humans*, 36(2): 252-265 (March 2006).

Carley, Kathleen and David Krackhardt. "A Typology for C2 Measures," Proceedings of the 1999 International Symposium on Command and Control Research and Technology. Newport RI (1999).

Carley, Kathleen and Jeff Reminga. *ORA: Organizational Risk Analyzer.* CMU-ISRI-04-101. Pittsburg, PA: CASOS, January 2004.

Carley, Kathleen, Jeffery Reminga and Natasha Kamneva. "Destabilizing Terrorist Networks," NAACSOS Conference Proceedings. Pittsburgh PA (2003).

Carley, Kathleen and Craig Schreiber. "Information Technology and Knowledge Distribution in C3I Teams," *Proceedings of the 2002 Command and Control Research and Technology Symposium.* Naval Postgraduate School, Monterey CA, 2002.

Champagne, Becky (Ed.) *Anatomy of a Terrorist Attack: An In-Depth Investigation into the 1998 Bombings of the US Embassies in Kenya and Tanzania.* Working Paper. Ridgway Center, International Security Studies. (Spring 2005) University of Pittsburg, Pittsburg PA. http://www.ridgway.pitt.edu/docs/working_papers/Anatomy%20v6--FINAL%20DOCUMENT.pdf (retrieved 1 March 2007)

Clark, Clinton. *Modeling and Analysis of Clandestine Networks*. MS Thesis, AFIT/GOR/ENS/05M-04. School of Engineering and Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2005.

Constenbader, Elizabeth and Thomas W. Valente. "The Stability of Centrality Measures When Networks are Sampled," *Social Networks*, 25: 283-307 (2005).

Department of Defense. *DoD Dictionary of Military Terms.* JP-1-02. Washington: Government Printing Office, 2001 (amended through January 2007). http://www.dtic.mil/doctrine/jel/doddict/ (retrieved: 15 February, 2007)

Department of State. *Patterns of Global Terrorism 2001*. Washington: Government Printing Office, May 2002.

Department of State. *Country Reports on Terrorism 2005*. Washington: Government Printing Office, April 2006.

Downs, Doneda. *Gauging the Commitment of Clandestine Members.* MS Thesis, AFIT/GOR/ENS/06M-06. School of Engineering and Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2006.

Freeman, Linton C. "Centrality in social Networks: Conceptual Clarification," *Social Networks*, 1: 215-239 (1978/1979).

Granovetter, Mark S. "The Strength of Weak Ties," *American Journal of Sociology*, 78(6): 1360-1380 (1973).

Haimes, Yacov Y. *Risk Modeling, Assessment and Management* (2nd Edition). Hoboken, NJ: John Wiley and Sons Inc., 2004.

Hamill, Jonathan T. *Analysis of Layered Social Networks*. Air Force Institute of Technology (AU), Wright-Patterson AFB OH, September 2006 (ADA

Haythornthwaite, Caroline. "Social Network Analysis: An Approach and Technique for the Study of Information Exchange," *Library and Information Science Research,* 18: 323 – 342 (1996).

Herbranson, Travis. *Isolating Key Players in Clandestine Networks*. MS thesis, AFIT/GOR/ENS/07M-11. School of Engineering and Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2006.

Hoffman, Bruce. "The Logic of Suicide Terrorism," *Atlantic Monthly.* 291:5 (2003).

Høyland, Arnljot and Marvin Rausand. *System Reliability Theory*. New York: John Wiley and Sons Inc., 1994

Kaplan, Stanley and B. John Garrick. "On the Quantitative Definition of Risk," *Risk Analysis*, 1(1): 11-27 (1981).

Katz, Leo. "A New Status Index Derived from Sociometric Analysis," *Psychometrika,* 18(1): 39-43 (March 1953).

Kenney, Ralph. *Value-Focused Thinking: A Path to Creative Decisionmaking*. Cambridge, MA: Harvard University Press, 1992.

Kincaid, David and Ward Cheney. *Numerical Analysis; Mathematics of Scientific Computing* (3rd Edition). Pacific Grove CA: Brooks|Cole, 2002.

Kirkwood, Craig. *Strategic Decision Making – Multiobjective Decision Analysis with Spreadsheets*. Belmont CA: Duxbury Press, 1997.

Klerks, Peter. "The Network Paradigm Applied to Criminal Organisations," *Connections,* 24(3): 53-65 (Winter 2001).

Krebs, Valdis E. "Mapping Networks of Terrorist Cells," *Connections*, 24 (3): 43-52 (2002).

Maples, Michael D., U. S. Army Director, Defense Intelligence Agency. "Current and Projected National Security Threats to the United States." Statement for the Record Senate Select Committee on Intelligence. 11 January, 2007.

McCormick, G. H. and G. Owen. "Security and Coordination in a Clandestine Organization," *Mathematical and Computer Modelling,* 31: 175-192 (2000).

Moghaddam, Fathali M. *From the Terrorists' Point of View: What They Experience and Why They Come to Destroy.* Westport, Connecticut: Praeger Security International General Interest, 2006.

Multi-National Forces-Iraq. *Fight for Freedom: Terrorist Tactics* (4 January, 2007). url: http://www.mnf-iraq.com/index.php?option=com_content&task=view&id=727&Itemid=44 (retrieved: 26 February, 2007)

Newman, M. E. J. "Analysis of Weighted Networks," *Physical Review E,* 70(2): 056131.1-506131.9 (November 2004).

National Defense University, Institute for National Strategic Studies. "Chapter 16: Transnational Trends - New Threats?" *Strategic Assessment 1999: Priorities for a Turbulent World.* Washington DC: National Defense University, Institute for National Strategic Studies (1999).

OPOTUS. *National Strategy for Combating Terrorism.* Washington: Government Printing Office, February 2003.

OPOTUS. *National Strategy for Combating Terrorism.* Washington: Government Printing Office, September 2006.

Papazoglou, Ioannis A. "Mathematical Foundations of Event Trees," *Reliability Engineering and System Safety,* 61: 169-183 (1998).

Pape, Robert A. "The Strategic Logic of Suicide Terrorism." American Political Science Review, 97:343-361 (2003)

Pottonen, Liisa. *A Method for the Probabilistic Security Analysis of Transmission Grids.* PhD dissertation. Helsinki University of Technology, Espoo, Finland, 2005.

Post, Jerrold (ed.). *Military Studies in the Jihad Against the Tyrants: The al-Qaeda Training Manual*. Maxwell AFB AL: Government Printing Office, 2005.

Ressler, Steve. "Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research," *Homeland Security Affairs*, II(2): 1-10 (July 2006).

Sabidussi, Gert. "The Centrality Index of a Graph," *Psychometrika,* 31(4): 581-603 (December 1966).

Sade, Donald S. "Sociometrics of Macaca Mulatta III: n-Path Centrality in Grooming Networks," *Social Networks* 11: 273-292 (1989).

Sageman, Marc. *Understanding Terror Networks*. University of Pennsylvania Press, 2004.

Sanderson, Thomas M. "Transnational Terror and Organized Crime: Blurring the Lines," *SAIS Review, XXIV*, 1: 49-61 (Winter-Spring 2004)

Seder, Joshua. *Testing Clandestine Social Network Formation for Statistical Significance Based on Nodal Attributes.* MS Thesis, AFIT/GOR/ENS/07M-24. School of Engineering and Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2006.

Shtub, Avraham, Jonathan F. Bard and Shlomo Globerson. *Project Management: Processes, Methodology and Economics (2nd Edition).* Upper Saddle River NJ: Pearson Prentice Hall, 2005.

Stanislawski, Bartosz and Margaret Hermann. "Transnational Organized Crime, Terrorism and WMD." *International Studies Review, 7(1): 158-160 (March 2005).*

Stephenson, Karen and Marvin Zelen. "Rethinking Centrality: Methods and Examples," *Social Networks*, 11: 1-37 (1989).

Stewart, Theodor J. "A Multi-Criteria Decision Support System for R&D Project Selection," *Journal of Operational Research Society,* 42(1):17-26 (January 1991).

Takeyh, Ray and Nikolas Gvosdev. "Do Terrorists Need a Home?," *The Washington Quarterly*, 25 (3): 97-108 (Summer 2002).

Taylor, Michael. "Influence Structures," *Sociometry*, 32(4): 490-502 (December 1969)

Tichy, Noel, Michael L. Tushman and Charles Fombrun. "Social Network Analysis for Organizations," *The Academy of Management Review*, 4(4): 507-519 (October 1979).

US Army Training and Doctrine Command (USTRADOC). *A Military Guide to Terrorism in the Twenty-First Century.* TRADOC DCSINT Handbook No.1. Fort Leavenworth KS August 2005.

van der Boorst, M. and H. Schoonakker. "An Overview of PSA Importance Measures," *Reliability Engineering and System Safety,* 72: 241-245 (2001).

Vesely, W., T. C. Davis, R. S. Denning and N. Saltos. *Measures of Risk Importance and Their Applications*. NUREG/CR-3385, US Nuclear Regulatory Commission (1983).

von Winderfeldt, Detlof and Ward Edwards. *Decision Analysis and Behavioral Research. Cambridge UK: Cambridge University Press, 1986.*

Wasserman, Stanley and Katherine Faust. *Social Network Analysis.* Cambridge UK: Cambridge University Press, 1994.

West, Douglas B. *Introduction to Graph Theory (2nd Edition).* Upper Saddle River NJ: Pearson Prentice Hall, 2001.

Vita

Captain Jennifer L. Geffre graduated from Highlands Ranch High School, Highlands Ranch, CO. She completed a Bachelor of Science in Mathematics with an emphasis in education from Colorado State University, Fort Collins, CO in December 1998. Upon graduation, she taught high school Mathematics at Highlands Ranch HS and ThunderRidge HS, Highlands Ranch, CO. She was commissioned into the US Air Force through 24th Training Squadron, Officer Training School at Maxwell AFB, Alabama.

Captain Geffre's first assignment was to the 453rd Electronic Warfare Squadron, as an Electronic Warfare System Analyst in March 2003. While in support of the Global Garrison Support Center (G2SC), she completed near-real time and real time tailored Information Operations analyses in support of Operations Enduring Freedom and Iraqi Freedom. In August 2005, she was competitively selected to study Operations Research at the Air Force Institute of Technology, Graduate School of Engineering and Management. Upon graduation, she will be assigned to Air Force Headquarters A-9 Studies and Analysis, Rosslyn, VA.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
05-03-2007	**Master's Thesis**	Aug 2005 – Mar 2007

4. TITLE AND SUBTITLE

A Layered Social and Operational Network Analysis

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Geffre, Jennifer L., Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Street, Building 642
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GOR/ENS/07-07

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/HECS
Attn: Gregory D. Sullivan, 2Lt, USAF
2689 G Street
WPAFB OH 45433-7022 DSN: 785-8015

NASIC/FCEB
Attn: Billy D. Darnell, Major, USAF
4180 Watson Way
WPAFB OH 45433-5648 DSN: 986-1023

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

To provide maximal disruption to a clandestine/terrorist network's ability to conduct missions, we must develop a means to determine the individuals' importance to the network and operations. In a network centric world, this importance is represented as an additive value of their criticality across the convergence of multiple layers of network connections. The connections layers of the network are comprised of social layers (Acquaintance, Friendship, Nuclear Family, Relatives, Student-Teacher, and Religious Mentors, Reverent Power and others), as well as layers representing interactions involving Resources, Knowledge/Skills and Temporal Local. The social criticality of an individual is measured by centrality. Event Trees and Risk Importance Measures are often used in a system reliability analysis to determine critical elements in the success or failure of operations. The inclusion of time and location importance will be determined by the observation of various group members at that local. The synergy gained from the application of these concepts to terror groups can be used to identify critical locations, resources and knowledge to their operations and can then be attributed to individuals connected to those essential elements. The combination of social and operational criticality can then be used to identify individuals whose removal or influence would disrupt or diminish network operations.

15. SUBJECT TERMS

Social Network Analysis, Risk Analysis, Eigenvector, Event Tree, System Reliability, Risk Importance Measures, Terrorism, al-Qaeda, Africa

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Richard F. Deckro, PhD (ENS)
U	U	U	UU	114	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-6565, ext 4325; e-mail: Richard.Deckro@afit.edu

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18